Computer Hacking Forensic Investigator v4

Course Outline

Module 01: Computer Forensics in Today's World

- Forensic Science
- Computer Forensics
    - Security Incident Report
    - Aspects of Organizational Security
    - Evolution of Computer Forensics
    - Objectives of Computer Forensics
    - Need for Computer Forensics
    - Benefits of Forensic Readiness
    - Goals of Forensic Readiness
    - Forensic Readiness Planning
- Cyber Crime
    - Cybercrime
    - Computer Facilitated Crimes
    - Modes of Attacks
    - Examples of Cyber Crime
    - Types of Computer Crimes
    - How Serious were Different Types of Incident?
    - Disruptive Incidents to the Business
    - Time Spent Responding to the Security Incident
    - Cost Expenditure Responding to the Security Incident
- Cyber Crime Investigation
    - Cyber Crime Investigation
    - Key Steps in Forensic Investigation
    - Rules of Forensics Investigation
    - Need for Forensic Investigator

    - Role of Forensics Investigator
    - Accessing Computer Forensics Resources
    - Role of Digital Evidence
    - Understanding Corporate Investigations
    - Approach to Forensic Investigation: A Case Study
    - When an Advocate Contacts the Forensic Investigator, He Specifies How to Approach the Crime Scene
    - Where and When do you Use Computer Forensics
- Enterprise Theory of Investigation (ETI)
- Legal Issues
- Reporting the Results

Module 02: Computer Forensics Investigation Process

- Investigating Computer Crime
    - Before the Investigation
    - Build a Forensics Workstation
    - Building Investigating Team
    - People Involved in Performing Computer Forensics
    - Review Policies and Laws
    - Forensics Laws
    - Notify Decision Makers and Acquire Authorization
    - Risk Assessment
    - Build a Computer Investigation Toolkit
- Computer Forensic Investigation Methodology
    - Steps to Prepare for a Computer Forensic Investigation
    - Obtain Search Warrant
        - Example of Search Warrant
        - Searches Without a Warrant
    - Evaluate and Secure the Scene
        - Forensic Photography
        - Gather the Preliminary Information at Scene
        - First Responder
    - Collect the Evidence
        - Collect Physical Evidence
            - Evidence Collection Form
        - Collect Electronic Evidence
        - Guidelines in Acquiring Evidences

- Secure the Evidence
    - Evidence Management
    - Chain of Custody
- Acquire the Data
    - Duplicate the Data (Imaging)
    - Verify Image Integrity
    - Recover Lost or Deleted Data
- Analyze the Data
    - Data Analysis
    - Data Analysis Tools
- Assess Evidence and Case
    - Evidence Assessment
    - Case Assessment
    - Processing Location Assessment
    - Best Practices
- Prepare the Final Report
    - Documentation in Each Phase
    - Gather and Organize Information
    - Writing the Investigation Report
    - Sample Report
- Testify in the Court as an Expert Witness
    - Expert Witness
    - Testifying in the Court Room
    - Closing the Case
    - Maintaining Professional Conduct
    - Investigating a Company Policy Violation
    - Computer Forensics Service Providers

Module 03: Searching and Seizing of Computers

- Searching and Seizing Computers without a Warrant
    - Searching and Seizing Computers without a Warrant
    - § A: Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers: General Principles
    - § A.1: Reasonable Expectation of Privacy in Computers as Storage Devices
    - § A.3: Reasonable Expectation of Privacy and Third-Party Possession
    - § A.4: Private Searches

- § A.5 Use of Technology to Obtain Information
- § B: Exceptions to the Warrant Requirement in Cases Involving Computers
- § B.1: Consent
- § B.1.a: Scope of Consent
- § B.1.b: Third-Party Consent
- § B.1.c: Implied Consent
- § B.2: Exigent Circumstances
- § B.3: Plain View
- § B.4: Search Incident to a Lawful Arrest
- § B.5: Inventory Searches
- § B.6: Border Searches
- § B.7: International Issues
- § C: Special Case: Workplace Searches
- § C.1: Private Sector Workplace Searches
- § C.2: Public-Sector Workplace Searches

- Searching and Seizing Computers with a Warrant
  - Searching and Seizing Computers with a Warrant
  - A: Successful Search with a Warrant
  - A.1: Basic Strategies for Executing Computer Searches
  - § A.1.a: When Hardware Is Itself Contraband, Evidence, or an Instrumentality or Fruit of Crime
  - § A.1.b: When Hardware is Merely a Storage Device for Evidence of Crime
  - § A.2: The Privacy Protection Act
  - § A.2.a: The Terms of the Privacy Protection Act
  - § A.2.b: Application of the PPA to Computer Searches and Seizures
  - § A.3: Civil Liability Under the Electronic Communications Privacy Act (ECPA)
  - § A.4: Considering the Need for Multiple Warrants in Network Searches
  - § A.5: No-Knock Warrants
  - § A.6: Sneak-and-Peek Warrants
  - § A.7: Privileged Documents
  - § B: Drafting the Warrant and Affidavit
  - § B.1: Accurately and Particularly Describe the Property to be Seized in the Warrant and/or Attachments to the Warrant
  - § B.1.a: Defending Computer Search Warrants Against Challenges Based on the Description of the “Things to be Seized”
  - § B.2: Establish Probable Cause in the Affidavit
  - § B.3: In the Affidavit Supporting the Warrant, Include an Explanation of the Search Strategy as Well as the Practical & Legal Considerations That Will Govern the Execution of the Search

- § C: Post-Seizure Issues
- § C.1: Searching Computers Already in Law Enforcement Custody
- § C.2: The Permissible Time Period for Examining Seized Computers
- § C.3: Rule 41(e) Motions for Return of Property

- The Electronic Communications Privacy Act
  - § The Electronic Communications Privacy Act
  - § A. Providers of Electronic Communication Service vs. Remote Computing Service
  - § B. Classifying Types of Information Held by Service Providers
  - § C. Compelled Disclosure Under ECPA
  - § D. Voluntary Disclosure
  - § E. Working with Network Providers
- Electronic Surveillance in Communications Networks
  - Electronic Surveillance in Communications Networks
  - § A. Content vs. Addressing Information
  - B. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127
  - C. The Wiretap Statute (“Title III”), 18 U.S.C. §§ 2510-2522
  - § C.1: Exceptions to Title III
  - § D. Remedies For Violations of Title III and the Pen/Trap Statute
- Evidence
  - Evidence
  - § A. Authentication
  - § B. Hearsay
  - § C. Other Issues
  - End Note

Module 04: Digital Evidence

- Digital Data
  - Definition of Digital Evidence
  - Increasing Awareness of Digital Evidence
  - Challenging Aspects of Digital Evidence
  - The Role of Digital Evidence
  - Characteristics of Digital Evidence
  - Fragility of Digital Evidence
  - Anti-Digital Forensics (ADF)
  - Types of Digital Data
  - Rules of Evidence
  - Best Evidence Rule

  - Federal Rules of Evidence
  - International Organization on Computer Evidence (IOCE)
  - http://www.ioce.org/
  - IOCE International Principles for Digital Evidences
  - SWGDE Standards for the Exchange of Digital Evidence
- Electronic Devices: Types and Collecting Potential Evidence
  - Electronic Devices: Types and Collecting Potential Evidence
- Evidence Assessment
  - Digital Evidence Examination Process
  - Evidence Assessment
  - Prepare for Evidence Acquisition
- Evidence Acquisition
  - Preparation for Searches
  - Seizing the Evidences
  - Imaging
  - Bit-stream Copies
  - Write Protection
  - Evidence Acquisition
  - Acquiring Evidence from Storage Devices
  - Collecting the Evidence
  - Collecting the Evidence from RAM
  - Collecting Evidence from Stand-Alone Network Computer
  - Chain of Custody
  - Chain of Evidence Form
- Evidence Preservation
  - Preserving Digital Evidence: Checklist
  - Preserving Floppy and Other Removable Media
  - Handling Digital Evidence
  - Store and Archive
  - Digital Evidence Findings
- Evidence Examination and Analysis
  - Evidence Examination
  - Physical Extraction
  - Logical Extraction
  - Analyze Host Data
  - Analyze Storage Media
  - Analyze Network Data

  - Analysis of Extracted Data
  - Timeframe Analysis
  - Data Hiding Analysis
  - Application and File Analysis
  - Ownership and Possession
- Evidence Documentation and Reporting
  - Documenting the Evidence
  - Evidence Examiner Report
  - Final Report of Findings
  - Computer Evidence Worksheet
  - Hard Drive Evidence Worksheet
  - Removable Media Worksheet
- Electronic Crime and Digital Evidence Consideration by Crime Category

Module 05: First Responder Procedures

- Electronic Evidence
- First Responder
- Role of First Responder
- Electronic Devices: Types and Collecting Potential Evidence
- First Responder Toolkit
  - First Responder Toolkit
  - Creating a First Responder Toolkit
  - Evidence Collecting Tools and Equipment
- First Response Basics
  - First Responder Rule
  - Incident Response: Different Situations
  - First Response for System Administrators
  - First Response by Non-Laboratory Staff
  - First Response by Laboratory Forensic Staff
- Securing and Evaluating Electronic Crime Scene
  - Securing and Evaluating Electronic Crime Scene: A Check-list
  - Warrant for Search & Seizure
  - Planning the Search & Seizure
  - Initial Search of the Scene
  - Health and Safety Issues
- Conducting Preliminary Interviews

- Questions to ask When Client Calls the Forensic Investigator
    - Consent
    - Sample of Consent Search Form
    - Witness Signatures
    - Conducting Preliminary Interviews
    - Conducting Initial Interviews
    - Witness Statement Checklist
- Documenting Electronic Crime Scene
    - Documenting Electronic Crime Scene
    - Photographing the Scene
    - Sketching the Scene
- Collecting and Preserving Electronic Evidence
    - Collecting and Preserving Electronic Evidence
    - Order of Volatility
    - Dealing with Powered OFF Computers at Seizure Time
    - Dealing with Powered ON Computers at Seizure Time
    - Dealing with Networked Computer
    - Dealing with Open Files and Startup Files
    - Operating System Shutdown Procedure
    - Computers and Servers
    - Preserving Electronic Evidence
    - Seizing Portable Computers
    - Switched ON Portables
- Packaging and Transporting Electronic Evidence
    - Evidence Bag Contents List
    - Packaging Electronic Evidence
    - Exhibit Numbering
    - Transporting Electronic Evidence
    - Handling and Transportation to the Forensics Laboratory
    - Storing Electronic Evidence
    - Chain of Custody
- Reporting the Crime Scene
- Note Taking Checklist
- First Responder Common Mistakes

Module 06: Incident Handling

- What is an Incident?

- Security Incidents
- Category of Incidents
  - Category of Incidents: Low Level
  - Category of Incidents: Mid Level
  - Category of Incidents: High Level
- Issues in Present Security Scenario
- How to identify an Incident?
- How to prevent an Incident?
- Defining the Relationship between Incident Response, Incident Handling, and Incident Management
- Incident Management
  - Incident Management
  - Threat Analysis and Assessment
  - Vulnerability Analysis
  - Estimating Cost of an Incident
  - Change Control
- Incident Reporting
  - Incident Reporting
  - Computer Incident Reporting
  - Whom to Report an Incident?
  - Report a Privacy or Security Violation
  - Preliminary Information Security Incident Reporting Form
  - Why don't Organizations Report Computer Crimes?
- Incident Response
  - Respond to a Security Incident
  - Security Incident Response (Detailed Form)
  - Incident response policies
  - Incident Response Checklist
  - Response Handling Roles
  - Incident Response: Roles and Responsibilities
    - SSM
    - ISSM
    - ISSO
  - Contingency/Continuity of Operations Planning
  - Budget/Resource Allocation
- Incident Handling
  - Handling Incidents

- Procedure for Handling Incident
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up
- Post-Incident Activity
- Education, Training, and Awareness
- Post Incident Report
- Procedural and Technical Countermeasures
- Vulnerability Resources

- CSIRT
  - What is CSIRT?
  - CSIRT: Goals and Strategy
  - CSIRT Vision
  - Motivation behind CSIRTs
  - Why does an Organization need an Incident Response Team?
  - Who works in a CSIRT?
  - Staffing your Computer Security Incident Response Team: What are the Basic Skills Needed?
  - Team Models
    - Delegation of Authority
  - CSIRT Services can be Grouped into Three Categories:
  - CSIRT Case Classification
  - Types of Incidents and Level of Support
  - Service Description Attributes
  - Incident Specific Procedures-I (Virus and Worm Incidents)
  - Incident Specific Procedures-II (Hacker Incidents)
  - Incident Specific Procedures-III (Social Incidents, Physical Incidents)
  - How CSIRT handles Case: Steps
  - US-CERT Incident Reporting System
  - CSIRT Incident Report Form
  - CERT(R) Coordination Center: Incident Reporting Form
  - Example of CSIRT
  - Best Practices for Creating a CSIRT
    - Step 1: Obtain Management Support and Buy-in
    - Step 2: Determine the CSIRT Development Strategic Plan

        - Step 3: Gather Relevant Information
        - Step 4: Design your CSIRT Vision
        - Step 5: Communicate the CSIRT Vision
        - Step 6: Begin CSIRT Implementation
        - Step 7: Announce the CSIRT
    - Limits to Effectiveness in CSIRTs
    - Working Smarter by Investing in Automated Response Capability
- World CERTs
    - World CERTs
    - Australia CERT (AUSCERT)
    - Hong Kong CERT (HKCERT/CC)
    - Indonesian CSIRT (ID-CERT)
    - Japan CERT-CC (JPCERT/CC)
    - Singapore CERT (SingCERT)
    - Taiwan CERT (TWCERT)
    - China CERT (CNCERT/CC)
    - CERT-CC
    - US-CERT
    - Canadian Cert
    - Forum of Incident Response and Security Teams
    - CAIS
    - NIC BR Security Office Brazilian CERT
    - EuroCERT
    - FUNET CERT
    - DFN-CERT
    - JANET-CERT
    - http://www.first.org/about/organization/teams/
    - http://www.apcert.org/about/structure/members.html
    - IRTs Around the World

Module 07: Computer Forensics Lab

- Setting a Computer Forensics Lab
    - Computer Forensics Lab
    - Planning for a Forensics Lab
    - Budget Allocation for a Forensics Lab
    - Physical Location Needs of a Forensic Lab
    - Structural Design Considerations

    - Environmental Conditions
    - Electrical Needs
    - Communication Needs
    - Work Area of a Computer Forensics Lab
    - Ambience of a Forensic Lab
    - Ambience of a Forensic Lab: Ergonomics
    - Physical Security Recommendations
    - Fire-Suppression Systems
    - Evidence Locker Recommendations
    - Computer Forensics Investigator
    - Law Enforcement Officer
    - Forensic Lab Licensing Requisite
    - Features of the Laboratory Imaging System
    - Technical Specification of the Laboratory-based Imaging System
    - Forensics Lab
    - Auditing a Computer Forensics Lab
    - Recommendations to Avoid Eyestrain
    - Computer Forensic Labs, Inc
    - Procedures at Computer Forensic Labs (CFL), Inc
    - Data Destruction Industry Standards
    - Case Study: San Diego Regional Computer Forensics Laboratory (RCFL)
- Hardware Requirements
    - Equipment Required in a Forensics Lab
    - Forensic Workstations
    - Basic Workstation Requirements in a Forensic Lab
    - Stocking the Hardware Peripherals
        - Paraben Forensics Hardware
            - Handheld First Responder Kit
            - Wireless StrongHold Bag
            - Remote Charger
            - Device Seizure Toolbox
            - Wireless StrongHold Tent
            - Passport StrongHold Bag
            - Project-a-Phone
            - SATA Adaptor Male/ Data cable for Nokia 7110/6210/6310/i
            - Lockdown
            - SIM Card Reader/ Sony Client N & S Series Serial Data Cable

        - CSI Stick
        - Portable USB Serial DB9 Adapter

    - Portable Forensic Systems and Towers
        - Forensic Air-Lite VI MKII laptop
        - Portable Forensic Systems and Towers: Original Forensic Tower II
        - Portable Forensic Systems and Towers: Portable Forensic Workhorse V
        - Portable Forensic Workhorse V: Tableau 335 Forensic Drive Bay Controller
        - Portable Forensic Systems and Towers: Forensic Air-Lite IV MK II
        - Portable Forensic Systems and Towers: Forensic Tower II
    - Forensic Write Protection Devices and Kits: Ultimate Forensic Write Protection Kit
    - Tableau T3u Forensic SATA Bridge Write Protection Kit
    - Tableau T8 Forensic USB Bridge Kit/Addonics Mini DigiDrive READ ONLY 12-in-1 Flash Media Reader
    - Tableau TACC 1441 Hardware Accleerator
    - Multiple TACC1441 Units
    - Digital Intelligence Forensic Hardware
        - FRED SR (Dual Xeon)
        - FRED-L
        - Forensic Recovery of Evidence Data Center (FREDC)
        - Rack-A-TACC
        - FREDDIE
        - UltraKit
        - UltraBay
        - UltraBlock
        - Micro Forensic Recovery of Evidence Device (µFRED)
    - Wiebetech
        - Forensics DriveDock
        - Forensics UltraDock v4
        - Drive eRazer
        - v4 Combo Adapters
        - ProSATA SS8
        - HotPlug
    - CelleBrite UFED System
    - DeepSpar:
        - Disk Imager Forensic Edition
        - 3D Data Recovery

        - Phase 1 Tool: PC-3000 Drive Restoration system:
        - Phase 2 Tool: DeepSpar Disk Imager
        - Phase 3 Tool: PC-3000 Data Extractor
    - InfinaDyne Forensic Products
        - Robotic Loader Extension for CD/DVD Inspector
        - Rimage Evidence Disc System
    - CD DVD Forensic Disc Analyzer with Robotic Disc Loader
    - Image MASSter
        - RoadMASSter- 3
        - Image MASSter --Solo-3 Forensic
        - Image MASSter –WipeMASSter
        - Image MASSter –DriveLock
        - Image MASSter: Serial-ATA DriveLock Kit USB/1394B
        - Image MASSter: DriveLock Firewire/USB
        - Image MASSter: DriveLock IDE
        - Image MASSter: DriveLock In Bay
    - Logicube:
        - Forensic MD5
        - Forensic Talon ®
        - RAID I/O Adapter ™
        - GPStamp™
        - Portable Forensic Lab™
        - CellDEK ®
        - Omniport
        - Desktop write PROtects
        - USB adapters
        - Adapters
        - Cables
    - Power Supplies and Switches
    - DIBS Mobile Forensic Workstation
    - DIBS Advanced Forensic Workstation
    - DIBS® RAID: Rapid Action Imaging Device
    - Forensic Archive and Restore Robotic Devices: Forensic Archive and Restore (FAR Pro)
- Software Requirements
    - Basic Software Requirements in a Forensic Lab
    - Maintain Operating System and Application Inventories

- Paraben Forensics Software: Device Seizure
- Paraben Hard Drive Forensics: P2 Commander
- Crucial Vision
- Paraben Hard Drive Forensics: P2 eXplorer
- InfinaDyne Forensic Products
    - CD/DVD Inspector
    - AccuBurn-R for CD/DVD Inspector
    - Flash Retriever Forensic Edition
    - ThumbsDisplay
- TEEL Technologies SIM Tools
    - SIMIS
    - SIMulate
    - SIMgen
- LiveDiscover™ Forensic Edition
- Tools: LiveWire Investigator

Module 08: Understanding Hard Disks and File Systems

- Hard Disk
    - Disk Drive Overview
    - Physical Structure of Hard Disk
    - Logical Structure of Hard Disk
    - Types of Hard Disk Interfaces
        - Types of Hard Disk Interfaces: SCSI
        - Types of Hard Disk Interfaces: IDE/EIDE
        - Types of Hard Disk Interfaces: USB
        - Types of Hard Disk Interfaces: ATA
        - Types of Hard Disk Interfaces: Fibre Channel
    - Disk Platter
    - Tracks
    - Tracks Numbering
    - Sector
    - Sector Addressing
    - Cluster
        - Cluster Size
        - Slack Space
        - Lost Clusters

        - Bad Sector
        - Disk Capacity Calculation
        - Measuring the Performance of Hard Disk

- Disk Partitions
    - Disk Partitions
    - Master Boot Record
- Boot Process
    - Windows XP System Files
    - Windows Boot Process (XP/2003)
    - http://www.bootdisk.com
- File Systems
    - Understanding File Systems
    - Types of File Systems
    - List of Disk File Systems
    - List of Network File Systems
    - List of Special Purpose File Systems
    - Popular Linux File Systems
    - Sun Solaris 10 File System: ZFS
    - Mac OS X File System
    - Windows File Systems
    - CD-ROM / DVD File System
    - Comparison of File Systems
- FAT32
    - FAT
    - FAT Structure
    - FAT32
- NTFS
    - NTFS
    - NTFS Architecture
    - NTFS System Files
    - NTFS Partition Boot Sector
    - NTFS Master File Table (MFT)
    - NTFS Metadata File Table (MFT)
    - Cluster Sizes of NTFS Volume
    - NTFS Files and Data Storage
    - NTFS Attributes
    - NTFS Data Stream

  - NTFS Compressed Files
  - NTFS Encrypted File Systems (EFS)
  - EFS File Structure
  - EFS Recovery Key Agent
  - EFS Key
  - Deleting NTFS Files
  - Registry Data
  - Examining Registry Data
  - FAT vs. NTFS
- Ext3
  - Ext2
  - Ext3
- HFS and CDFS
  - HFS
  - CDFS
- RAID Storage System
  - RAID Storage System
  - RAID Levels
  - Recover Data from Unallocated Space using File Carving Process
- Hard Disk Evidence Collector Tools
  - Evidor
  - WinHex
  - Logicube: Echo PLUS
  - Logicube: Sonix
  - Logicube: OmniClone Xi
  - Logicube: OmniWipe
  - Logicube: CloneCard Pro
  - ImageMASSter: ImageMASSter 40008i
  - eDR Solutions: Hard Disk Crusher

Module 09: Digital Media Devices

- Digital Storage Devices
  - Digital Storage Devices
  - Magnetic Tape
  - Floppy Disk
  - Compact Disk
  - CD-ROM

- DVD
- DVD-R, DVD+R, and DVD+R(W)
- DVD-RW, DVD+RW
- DVD+R DL/ DVD-R DL/ DVD-RAM
- Blu-Ray
- Network Attached Storage (NAS)
- IPod
- Zune
- Flash Memory Cards
- Secure Digital (SD) Memory Card
- Secure Digital High Capacity (SDHC) Card
- Secure Digital Input Output (SDIO) Card
- Compact Flash (CF) Memory Card
- Memory Stick (MS) Memory Card
- Multi Media Memory Card (MMC)
- xD-Picture Card (xD)
- SmartMedia Memory (SM) Card
- Solid state drives
- Tape Libraries and Autoloaders
- Barracuda Hard Drives
- Hybrid Hard Drive
- Holographic Data Storage
- ExpressCard
- USB Flash Drives
- USB Flash in a Pen
- E-ball Futuristic Computer

- Different Models of Digital Devices
  - Different Types of Pocket Hard Drives
  - Different Types of Network-Attached Storage Devices
  - Different Types of Digital Camera Devices
  - Different Types of Mini Digital Cameras
  - Different Types of Digital Video Cameras
  - Different Types of Mobile Devices
  - Mobile Devices in the Future
  - Different Types of Digital Audio Players
  - Different Types of Digital Video Players
  - Different Types of Laptop computers

  - Solar Powered Concept for Laptop Gadget
  - Different Types of Bluetooth Devices
  - Different Types of USB Drives

Module 10: CD/DVD Forensics

- Compact Disk
- Types of CDs
- Digital Versatile Disk (DVD)
- DVD-R and DVD+R
- DVD-RW and DVD+RW
- DVD+R DL, DVD-R DL, DVD-RAM
- HD-DVD (High Definition DVD)
- HD-DVD
- Blu-Ray
- SID Code
- How Criminal uses CD/DVD for Crime
- Pre-Requisite for CD/DVD Forensics
- Steps for CD Forensics
  - Collect the CD/DVD Evidences
  - Precautions while Collecting the Evidences
  - Document the Scene
  - Preserve the Evidences
  - Create Image of CD/DVD
  - Recover Data from Damaged or Corrupted CDs/DVDs
  - Data Analysis
- Identify Pirated CD/DVDs
- Original and Pirated CD/DVDs
- CD/DVD Imaging Tools
  - UltraISO
  - MagicISO
  - Cdmage
  - Alcohol
  - Nero
- CD/DVD Data Recovery Tools
  - CDRoller
  - Badcopy Pro
  - Multi Data Rescue

- InDisk Recovery
- Stellar Phoenix -CD Data Recovery Software
- CD Recovery Toolbox
- IsoBuster
- CD/DVD Inspector
- Acodisc CD & DVD Data Recovery Services

Module 11: Windows Linux Macintosh Boot Process

- Terminologies
- Boot Loader
- Boot Sector
- Anatomy of MBR
- Windows Boot Sequence
- Linux Boot Sequence
- Macintosh Boot Sequence
- Windows XP Boot Process
  - Windows XP Boot Process
- Linux Boot Process
  - Common Startup Files in UNIX
  - List of Important Directories in UNIX
- Linux Boot Process Steps
  - Step 1: The Boot Manager
    - GRUB: Boot Loader
  - Step 2: init
    - Step 2.1: /etc/inittab
    - Run Levels
    - The Run Level Scripts
    - How Processes in Runlevels Start
    - The Run Level Actions
  - Step 3: Services
  - Step 4: More inittab
    - Operating Modes
- Macintosh Boot Process
  - Mac OS X
  - Mac OS X Hidden Files
  - Booting Mac OS X
  - Mac OS X Boot Options

    - The Mac OS X Boot Process

Module 12: Windows Forensics I

- Volatile Information
- Non-volatile Information
- Collecting Volatile Information
    - System Time
    - Logged-on-Users
    - Open Files
    - Net file Command
    - Psfile Tool
    - Openfiles Command
    - NetBIOS Name Table Cache
    - Network Connections
    - Netstat with the –ano Switch
- Netstat with the –r Switch
    - Process Information
    - Tlist Tool
    - Tasklist Command
    - Pslist Tool
    - Listdlls Tool
    - Handle Tool
    - Process-to-Port Mapping
    - Netstat Command
    - Fport Tool
    - Openports Tool
    - Network Status
    - Ipconfig Command
    - Promiscdetect Tool
    - Promqry Tool
    - Other Important Information
- Collecting Nonvolatile Information
    - Collecting Nonvolatile Information
    - Examining File Systems
    - Registry Settings
    - Microsoft Security ID
    - Event Logs

  - Index.dat File
  - Devices and Other Information
  - Slack Space
  - Virtual Memory
  - Tool: DriveSpy
  - Swap File
  - Windows Search Index
  - Tool: Search Index Examiner
  - Collecting Hidden Partition Information
  - Hidden ADS Streams
  - Investigating ADS Streams
- Windows Memory Analysis
  - Windows Memory Analysis
  - Importance of Memory Dump
  - EProcess Structure
  - Process Creation Mechanism
  - Parsing Memory Contents
  - Parsing Process Memory
  - Extracting the Process Image
  - Collecting Process Memory
- Windows Registry Analysis
  - Inside the Registry
  - Registry Contents
  - Registry Structure within a Hive File
  - Registry Analysis
  - System Information
  - Time Zone Information
  - Shares
  - Audit Policy
  - Wireless SSIDs
  - Autostart Locations
  - System Boot
  - User Login
  - User Activity
  - Enumerating Autostart Registry Locations
  - USB Removable Storage Devices
  - Mounted Devices

    - Finding Users
    - Tracking User Activity
    - The UserAssist Keys
    - MRU Lists
    - Search Assistant
    - Connecting to Other Systems
    - Analyzing Restore Point Registry Settings
    - Determining the Startup Locations
- Cache, Cookie and History Analysis
    - Cache, Cookie and History Analysis in IE
    - Cache, Cookie and History Analysis in Firefox/Netscape
    - Browsing Analysis Tool: Pasco
    - IE Cache View
    - Forensic Tool: Cache Monitor
    - Tool - IE History Viewer
    - IE Cookie Analysis
    - Investigating Internet Traces
    - Tool – IECookiesView
    - Tool- IE Sniffer
- MD5 Calculation
    - MD5 Calculation
    - MD5 Algorithm
    - MD5 Pseudocode
    - MD5 Generator: Chaos MD5
    - Secure Hash Signature Generator
    - MD5 Generator: Mat-MD5
    - MD5 Checksum Verifier 2.1
- Windows File Analysis
    - Recycle Bin
    - System Restore Points
    - Prefetch Files
    - Shortcut Files
    - Searching with Event Viewer
    - Word Documents
    - PDF Documents
    - Image Files
    - File Signature Analysis

    - NTFS Alternate Data Streams
    - Executable File Analysis
    - Documentation Before Analysis
    - Static Analysis Process
    - Search Strings
    - PE Header Analysis
    - Import Table Analysis
    - Export Table Analysis
    - Dynamic Analysis Process
    - Creating Test Environment
    - Collecting Information Using Tools
    - Dynamic Analysis Steps
- Metadata Investigation
    - Metadata
    - Types of Metadata
    - Metadata in Different File System
    - Viewing Metadata
    - MetaViewer
    - Metadata Analyzer
    - iScrub

Module 13: Windows Forensics II

- Text Based Log
    - Understanding Events
    - Event Record Structure
    - Vista Event Logs
    - IIS Logs
    - Parsing IIS Logs
    - Parsing FTP Logs
    - Parsing DHCP Server Logs
    - Parsing Windows Firewall Logs
    - Using the Microsoft Log Parser
- Other Audit Events
    - Evaluating Account Management Events
    - Examining Audit Policy Change Events
    - Examining System Log Entries
    - Examining Application Log Entries

- Forensic Analysis of Event Logs
  - Using EnCase to Examine Windows Event Log Files
  - Windows Event Log Files Internals
  - Window Password Issues
  - Understanding Windows Password Storage
  - Cracking Windows Passwords Stored on Running Systems
  - Exploring Windows Authentication Mechanisms
  - Sniffing and Cracking Windows Authentication Exchanges
  - Cracking Offline Passwords
- Forensics Tools
  - Helix
  - Tools Present in Helix CD for Windows Forensics
  - Helix Tool: SecReport
  - Helix Tool: Windows Forensic Toolchest (WFT)
  - Built-in Tool: Sigverif
  - Word Extractor
  - Registry Viewer Tool: RegScanner
  - Pmdump
  - System Scanner
  - Integrated Windows Forensics Software: X-Ways Forensics
  - Tool - Traces Viewer
  - Traces Viewer: Images
  - Traces Viewer: Pages
  - Traces Viewer: Other
  - Traces Viewer: Cookies
  - CD-ROM Bootable Windows XP
  - Ultimate Boot CD-ROM
  - List of Tools in UB CD-ROM

Module 14: Linux Forensics

- Introduction to Linux
  - Introduction of Linux OS
  - Linux Boot Sequence
  - File System in Linux
  - File System Description
  - Linux Forensics
  - Use of Linux as a Forensics Tool

    - Advantages of Linux in Forensics
    - Disadvantages of Linux in Forensics
    - Precautions During Investigation
    - Recognizing Partitions in Linux
    - Mount Command
    - dd command options
    - Floppy Disk Analysis
    - Hard Disk Analysis
- Data Collection
    - Forensic Toolkit Preparation
    - Data Collection using the Toolkit
    - Keyword Searching
    - Linux Crash Utility
    - Linux Crash Utility: Commands
        - Crash> ps
        - crash> ps -t
        - crash> ps –a
        - crash> foreach files
        - crash> foreach net
- Case Examples
    - Case Example I
        - Step-by-Step Approach to Case
        - Challenges In Disk Forensics With Linux
    - Case Example II
        - Jason Smith Case
        - Step-by-Step Approach to Case
- Linux Forensics Tools
    - Popular Linux Forensics Tools
        - The Sleuth Kit
        - Tools in “The Sleuth Kit”
    - Autopsy
        - The Evidence Analysis Techniques in Autopsy
            - File Listing
            - File Content
            - Hash Databases
            - File Type Sorting

        - Timeline of File Activity
        - Keyword Search
        - Meta Data Analysis
        - Data Unit Analysis
        - Image Details
- SMART for Linux
    - Features of SMART for Linux
- Penguin Sleuth
    - Tools Included in Penguin Sleuth Kit
- THE FARMAER'S BOOT CD
    - Delve
- Forensix
- Maresware
- Major Programs Present in Maresware
- Captain Nemo
- The Coroner's Toolkit (TCT)
- Tool: FLAG
- Tool: Md5deep
- Tool: TestDisk
- Tool: Vinetto

Module 15: Mac Forensics

- Mac OS and File Systems
    - Mac OS X
    - Partitioning Schemes
        - Apple Partition Map(APM)
        - Apple Partition Map Entry Record
        - GUID Partition Table
    - Mac OS X File System
        - HFS+ File System
    - Mac OS X Directory Structure
    - Mac Security Architecture Overview
- Mac Forensics: Collecting Evidence
    - Pre-requisites for Mac Forensics
    - Obtaining System Date and Time
    - Single User Mode
    - Determining and Resetting Open Firmware Password

- Checking Plist Files
- Collect User Home Directory Information
- Forensics Information in User Library Folder
- Collect User Accounts Information
- User IDs
- Gather user information from pllist files
- Use Spotlight for Keyword Search
- Collecting Information Regarding Parental Controls for Local Account
- File Vault and Mac OS X Security
- Cracking File Vault
- POSIX Permissions
  - Viewing POSIX Permissions
- Viewing ACL Permissions
- Mac OS X Log Files
- Locating iChat Configuration File
- Viewing iChat Logs
- Gathering Safari Information
- Checking Wi-Fi Support
- Checking Bluetooth Support
- Vulnerable Features of Mac

- Mac Forensics: Imaging
  - Imaging a Target Macintosh
    - Target Disk Mode
    - LiveCD Method
    - Drive Removal
  - Acquiring the Encrypted User Home Directory
  - .Mac and Related Evidence
  - Quick View Plus
  - Cover Flow
- Mac Forensics: Tools
  - gpart
  - MadLockPick
  - File Juicer
  - MacAnalysis
  - MacQuisition
  - FTK Imager
  - dd_rescue

  - md5deep
  - Foremost
  - Mac forensic lab
  - LinkMASSter

Module 16: Data Acquisition and Duplication

- Data Acquisition
  - Data Acquisition
  - Types of data acquisition systems
  - Determining the Best Acquisition Methods
  - Data Recovery Contingencies
  - Data Acquisition Mistakes
- Data Duplication
  - Issues with Data Duplication
  - Data Duplication in Mobile Multi-database System
  - Data Duplication System Used in USB Devices
  - Data Backup
- Data Acquisition Tools and Commands
  - MS-DOS Data Acquisition Tool: DriveSpy
    - Using Windows Data Acquisition Tools
    - FTK Imager
  - Acquiring Data on Linux
    - dd command
    - Extracting the MBR
    - Netcat Command
    - dd command(Windows XP Version)
    - Mount Image Pro
    - Snapshot Tool
  - Snapback DatArrest
    - Data Acquisition Toolbox
    - Data Acquisition Tool: SafeBack
  - Hardware Tool: Image MASSter Solo-3 Forensic
    - Image MASSter --RoadMASSter- 3
    - Image MASSter --WipeMASSter
    - Image MASSter –DriveLock
  - Hardware Tool: LinkMASSter-2

- Hardware Tool: RoadMASSter-2
- Logicube: ECHOPLUS & Sonix
- Logicube: OmniClone Xi series
- Logicube: OmniPORT
- Logicube: OmniWipe & Clone Card Pro
- Logicube: Forensic MD5
- Logicube: Forensic Talon
- Logicube: RAID I/O Adapter
- Logicube: GPStamp
- Logicube: Portable Forensic Lab
- Logicube: CellDEK
- Logicube: Desktop write PROtects
- Logicube: USB adapter
- Logicube: Adapters
- Logicube: Cables

- Data Duplication Tools
  - Data Duplication Tool: R-drive Image
  - Data Duplication Tool: DriveLook
  - Data Duplication Tool: DiskExplorer
  - Save-N-Sync
  - Hardware Tool: ImageMASSter 6007SAS
    - Hardware Tool: Disk Jockey IT
  - SCSIPAK
  - IBM DFSMSdss
  - Tape Duplication System: QuickCopy
  - DeepSpar: Disk Imager Forensic Edition
  - DeepSpar: 3D Data Recovery
  - Phase 1 Tool: PC-3000 Drive Restoration System
  - Phase 2 Tool: DeepSpar Disk Imager
  - Phase 3 Tool: PC-3000 Data Extractor
  - MacQuisition
  - Athena Archiver

Module 17: Recovering Deleted Files and Deleted Partitions

- Recovering Deleted Files
  - Deleting Files
  - What happens when a File is deleted in Windows?

- Recycle Bin in Windows
  - Storage Locations of Recycle Bin in FAT and NTFS System
  - How The Recycle Bin Works
- Damaged or Deleted INFO File
- Damaged Files in Recycled Folder
- Damaged Recycle Folder
- How to Undelete a File
- Data Recovery in Linux
- Tools to Recover Deleted Files
  - Tool: Search and Recover
  - Tool: Zero Assumption Digital Image Recovery
  - Tool: e2Undel
  - Tool: R-linux
  - Tool: O&O Unerase
  - Tool: Restorer 2000
  - Tool: Badcopy Pro
  - Tool: File Scavenger
  - Tool: Mycroft V3
  - Tool: PC ParaChute
  - Tool: Stellar Phoenix
  - Tool: Filesaver
  - Tool: Virtual Lab
  - Tool: Drive and Data Recovery
  - Tool: Active@ UNERASER - DATA Recovery
  - Tool: Restoration
  - Tool: PC Inspector File Recovery
  - Tool: PC Inspector Smart Recovery
  - Tool: Fundelete
  - Tool: RecoverPlus Pro
  - Tool: OfficeFIX
  - Tool: Recover My Files
  - Tool: Zero Assumption Recovery
  - Tool: SuperFile Recover
  - Tool: IsoBuster
  - Tool: CDRoller
  - Tool: DiskInternals Uneraser

- Tool: DiskInternal Flash Recovery
- Tool: DiskInternals NTFS Recovery
- Recover lost/deleted/corrupted files on CDs and DVDs
- Tool: Undelete
- Tool: Active@ UNDELETE
- Data Recovery Tool: CD Data Rescue
- Tool: File Recover
- Tool: WinUndelete
- Tool: R-Undelete
- Tool: Image Recall
- Tool: eIMAGE Recovery
- Tool: Recover4all Professional
- Tool: eData Unerase
- Tool: Easy-Undelete
- InDisc Recovery
- TOKIWA DataRecovery
- Data Recovery Wizard Professional
- CD Recovery Toolbox
- Smart Protector-Internet Eraser
- Active@ File Recovery
- SoftPerfect File Recovery
- Partition Recovery
- FinalRecovery
- Mutilate File Wiper
- Repair My Excel
- Repair Microsoft Word Files
- Zip Repair
- Canon RAW File Recovery Software

- Recovering Deleted Partitions
  - Deletion of Partition
  - Deletion of Partition using Windows
  - Deletion of Partition using Command Line
  - Recovery of Deleted Partition
  - Recovering Deleted Partition Tools
    - GetDataBack

    - DiskInternals Partition Recovery
    - Active@ Partition Recovery
    - Handy Recovery
    - Acronis Recovery Expert
    - Active@ Disk Image
    - TestDisk
    - Recover It All!
    - Scaven
    - Partition Table Doctor
    - NTFS Deleted Partition Recovery
    - Flash Retriever Forensic
    - ThumbsDisplay

Module 18: Forensics Investigations Using AccessData FTK

- Forensic Toolkit (FTK®)
- Features of FKT
- Installation of FTK
  - Software Requirement
  - Installing FTK
  - FTK Installation
  - Codemeter Stick Installation
  - Oracle Installation
  - Single Computer Installation
  - Choosing An Evidence Server
  - Installing the KFF Library
  - Installing on Separate Computers
- Starting with FTK
  - Starting FTK
  - Setting Up The Application Administrator
  - Case Manager Window
  - Toolbar Components
  - Properties Pane
  - Hex Interpreter Pane
  - Web Tab
  - Filtered Tab
  - Text Tab

- Hex Tab
- Explore Tab
- Quickpicks Filter
- Data Processing Status Dialog
- Overview Tab
- Email Tab
- Graphics Tab
- Thumbnails Pane
- Bookmarks Tab
- Live Search Tab
- Index Search Tab
- Creating Tabs
- Launching FKT

- Working with FTK
  - Creating A Case
  - Evidence Processing Options
  - Selecting Data Carving Options
  - Selecting Evidence Discovery Options
  - Selecting Evidence Refinement (Advanced) Options
  - Selecting Index Refinement (Advanced) Options
  - Refining an Index by File Date/Size
  - Adding Evidence
  - Backing Up the Case
  - Restoring a Case
  - Deleting a Case
- Working with Cases
  - Opening an Existing Case
  - Adding Evidence
  - Selecting a Language
  - Additional Analysis
  - Properties Tab
  - The Hex Interpreter Tab
  - Using The Bookmark Information Pane
  - Creating a Bookmark
  - Bookmarking Selected Text
  - Adding Evidence to an Existing Bookmark
  - Moving A Bookmark

  - Removing A Bookmark
  - Deleting Files From A Bookmark
  - Verifying Drive Image Integrity
  - Copying Information From FTK
  - Exporting File List Info
  - Exporting the Word List
  - Creating a Fuzzy Hash Library
  - Selecting Fuzzy Hash Options During Initial Processing
  - Additional Analysis Fuzzy Hashing
  - Comparing Files Using Fuzzy Hashing
  - Viewing Fuzzy Hash Results
- Searching a Case
  - Conducting A Live Search
  - Customizing The Live Search Tab
  - Documenting Search Results
  - Using Copy Special to Document Search Results
  - Bookmarking Search Results
- Data Carving
  - Data carving
  - Data Carving Files In An Existing Case
- Using Filters
  - Creating A Filter
  - Refining A Filter
  - Deleting A Filter
- Decrypting Encrypted Files
  - Decrypting Files And Folders
  - Viewing Decrypted Files
  - Decrypting Domain Account EFS Files
  - Decrypting Credant Files
  - Decrypting Safeguard Utimaco Files
- Working with Reports
- Creating A Report
  - Saving Settings
  - Entering Basic Case Information
  - Including Bookmarks
  - Including Graphics
  - Selecting a File Path List

- Selecting a File Properties List
- Registry Selections
- Selecting the Report Location
- HTML Case Report
- PDF Report

- Customizing the Interface
  - Creating Custom Tabs
  - Customizing File List Columns
  - Creating and Modifying Column Settings

Module 19: Forensics Investigations Using Encase

- Evidence File
- Verifying Evidence Files
- Evidence File Format
- Verifying File Integrity
- Hashing
- Acquiring Image
- Configuring EnCase
- View Menu
- Device Tab
- Viewing Files and Folders
- Bottom Pane
- Viewers in Bottom Pane
- Status Bar
- Searching
- Keywords
- Adding Keywords
- Grouping
- Add multiple Keywords
- Starting the Search
- Search Hits Tab
- Search Hits
- Bookmarks
- Creating Bookmarks
- Adding Bookmarks
- Bookmarking Selected Data
- Recovering Deleted Files/folders in FAT Partition

- Viewing Recovered Files
- Recovering Folders in NTFS
- Master Boot Record (MBR)
- Bookmark Data
- NTFS Starting Point
- Viewing Disk Geometry
- Recovering Deleted Partitions
- Hash Values
- Creating Hash Sets
- MD5 Hash
- Creating Hash
- Viewers
- Signature Analysis
- Viewing the Results
- Copy/UnErase Files and Folders
- Email Recovery
- Reporting
- IE Cache Images

Module 20: Steganography

- Steganography
- Model of Stegosystem
- Application of Steganography
- Classification of Steganography
    - Technical Steganography
    - Linguistic Steganography
- Digital Steganography Techniques
    - Injection
    - Least Significant Bit (LSB)
    - Transform Domain Techniques
    - Spread Spectrum Techniques
    - Perceptual Masking
- Cover Generation Technique
- Statistical Method Technique
- Distortion Technique
- Different Forms of Steganography

- Text File Steganography
- Image File Steganography
  - Steganography Technique in Image File
  - Least Significant Bit Insertion in Image Files
  - Process of Hiding Information in Image Files
  - Masking and Filtering in Image Files
  - Algorithms and Transformation
- Audio File Steganography
  - Low-bit Encoding in Audio Files
  - Phase Coding
  - Spread Spectrum
  - Echo Data Hiding
- Video File Steganography

- Steganographic File System
- Issues in Information Hiding
  - Levels of Visibility
  - Robustness vs. Payload
  - File Format Dependence
- Cryptography
- Model of Crypto System
- Steganography vs. Cryptography
- Public Key Infrastructure (PKI)
- Key Management Protocols
- Watermarking
  - What is Watermarking?
  - Case Study
  - Steganography vs. Watermarking
  - Types of Watermarks
    - Visible Watermarks
    - Invisible Watermarks
  - Working of Different Watermarks
  - Attacks on Watermarking
  - Application of Watermarking
  - Currency Watermarking
  - Digimarc's Digital Watermarking
  - Watermarking – Mosaic Attack

        - Mosaic Attack – Javascript code
        - 2Mosaic – Watermark breaking Tool
- Steganography Detection
    - How to Detect Steganography?
    - Detecting Steganography
    - Detecting Text, Image, Audio and Video Steganography
    - Counterfeit Detection
- Steganalysis
    - Steganalysis Methods/Attacks on Steganography
        - Attack Types
        - Stego Only Attack
        - Known Cover Attack
        - Known Message Attack
        - Known Stego Attack
        - Chosen Stego Attack
        - Disabling or Active Attack
        - Chosen Message Attack
        - Disabling or Active Attacks
        - Blur
        - Noise
        - Noise Reduction
        - Sharpen
        - Rotate
        - Resample
        - Soften
- Introduction to Stego-Forensics
- Steganography in the Future
- Hiding Information in DNA
- Unethical Use of Steganography
- TEMPEST
- Emissions Security (EMSEC)
- Van Eck phreaking
- Legal Use of Steganography
- Steganography Tools
    - S- Tools
    - Steghide

- Mp3Stego
- Invisible Secrets 4
- Stegdetect
- Steg Suite
- Stego Watch
- Snow
- Fort Knox
- Image Hide
- Blindside
- Camera/Shy
- Gifshuffle
- Data Stash
- JPHIDE and JPSEEK
- wbStego
- OutGuess
- Masker
- Cloak
- StegaNote
- Stegomagic
- Hermetic Stego
- StegSpy
- Stealth
- WNSTORM
- Xidie
- CryptArkan
- Info Stego
- Scramdisk
- Jpegx
- CryptoBola
- ByteShelter I
- Camuflage
- Stego Analyst
- Steganos
- Pretty Good Envelop
- Hydan
- EzStego
- Steganosaurus

    - appendX
    - Stego Break
    - Stego Hunter
    - StegParty
    - InPlainView
    - Z-File
    - MandelSteg and GIFExtract

Module 21: Image Files Forensics

- Common Terminologies
- Introduction to Image Files
    - Understanding Vector Images
    - Understanding Raster Images
    - Metafile Graphics
- Image File Formats
    - Understanding Image File Formats
        - GIF (Graphics Interchange Format)
        - JPEG (Joint Photographic Experts Group)
        - JPEG File Structure
        - JPEG 2000
        - BMP (Bitmap) File
        - BMP File Structure
        - PNG (Portable Network Graphics)
        - Tagged Image File Format (TIFF)
        - TIFF File Structure
        - ZIP (Zone Information Protocol)
    - Best Practices for Forensic Image Analysis
- Use MATLAB for Forensic Image Processing
    - Advantages of MATLAB
- Data Compression
    - How File Compression Works?
    - Understanding Data Compression
    - Huffman Coding Algorithm
    - Lempel-Ziv Coding Algorithm
    - Lossy Compression
    - Vector Quantization

- Locating and Recovering Image Files
    - Locating and Recovering Image Files
    - Analyzing Image File Headers
    - Repairing Damaged Headers
    - Reconstructing File Fragments
    - Identifying Unknown File Formats
    - Identifying Image File Fragments
        - http://www.filext.com
        - Picture Viewer: Ifran View
        - Picture Viewer: ACDsee
        - Picture Viewer: Thumbsplus
        - Picture Viewer: AD
        - Picture Viewer: Max
        - FastStone Image Viewer
        - XnView
        - Faces – Sketch Software
- Digital Camera Data Discovery Software: FILE HOUND
- http://vectormagic.com/
- Steganography in Image Files
- Steganalysis Tool
    - Hex Workshop
    - S-tools
    - Stegdetect
- Image File Forensic Tools
    - GFE Stealth (Graphics File Extractor)
    - ILook v8
    - P2 eXplorer
    - VisionStage
    - Digital Pictures Recovery
- Identifying Copyright Issues on Graphics
- Case Study

Module 22: Audio file forensics

- Audio Forensics
- Why audio forensics
- Use of voice as a tool
- Fast Fourier Transform (FFT)

- Methodologies of Audio Forensics
- Voice Identification
- Audibility Analysis
- Audio Enhancement
- Authenticity Analysis
- Sound Identification
- Event Sequence Analysis
- Dialogue decoding
- Remnant Signal Analysis
- Integrity Verification of the Audio
- Audio Forensics Process
  - Evidence handling
  - Preparation of Exemplars
  - Preparation of Copies
  - Preliminary Examination
  - Analog to Digital Conversion
    - Audio File Formats
  - Preparation of Spectrograms
  - Spectrographic Analysis
- Sound Spectrograph
- Sound Recordings As Evidence In Court Proceedings
- Audio File Manipulation
- Tools
  - DCLive Forensics
  - Zoom H2 Portable Digital Recorder
  - CEDAR for Windows
    - Console
    - Declick
    - Decrackle
    - DEHISS2
    - NR-3 v2
    - Phase Corrector
    - EQ and dynamics
    - Spectral analyzer
  - Audio File Forensic Tools
    - DCVST

        - Advanced audio corrector
        - Acoustica
        - Smaart
        - DNS1500 Dialogue Noise Suppressor
        - DNS2000 Dialogue Noise Suppressor
        - DNS 3000Dialogue Noise Suppressor
        - M-Audio MicroTrack 2496 Portable Digital Recorder
        - Cardinal
        - JBR 4 Channel Microcassette Playback/Transcriber Unit
        - JBR Universal DVD/CD Player/Transcriber Unit

Module 23: Video File Forensics

- Video File Forensics
- Crimes involving Video Files
- Need of Video File Forensics
- Video File Formats
- Pre-Requisite for Video Forensics
- Selecting Video Forensics Tools
- Precaution During Video File Forensics
- Preparing for Video Forensics
- Video Forensic Methodology
    - Frame Averaging
    - Video De-Multiplexing
    - De-multiplexing Tool: Video Active
    - dPlex Pro: De-multiplexing Tool
    - Video Stabilizing
    - Motion Deblurring
    - Magnifying and Color Correcting Video
    - Spotlighting the Particular Region
    - Audio Analysis
    - Performing Video Steganalysis
- StegSecret
- UQLIPS: Near Duplicate Video Clip Detection System
- Analysis of Output
- Video Forensics Tools
    - dTective

    - VideoFOCUS
    - Sarensix Video Forensic Services
    - Audio Video Forensic Lab (AVFL)
    - VideoDetective
    - Jam
    - Ikena Reveal

Module 24: Application Password Crackers

- Password - Terminology
- What is a Password Cracker?
- How Does a Password Cracker Work?
- Various Password Cracking Methods
    - Brute Force Attack
        - Brute Force Attack Time Estimator
    - Dictionary Attack
    - Syllable Attack/Rule-based Attack/Hybrid Attack
    - Password Guessing
    - Rainbow Attack
        - Time Needed to Crack Passwords
- Classification of Cracking Software
    - System Level Password Cracking
    - CMOS Level Password Cracking
        - Tool: Cmospwd
        - ERD Commander
        - Active Password Changer
    - Application Software Password Cracker
    - Distributed Network Attack
    - Passware Kit
    - Accent Keyword Extractor
    - Advanced Zip Password Recovery
- Default Password Database
    - http://phenoelit.darklab.org/
    - http://www.defaultpassword.com/
    - http://www.cirt.net/cgi-bin/passwd.pl
    - http://www.virus.org/index.php?
- Pdf Password Crackers
- Password Cracking Tools

- Cain & Abel
- LCP
- SID&User
- Ophcrack 2
- John the Ripper
- Netscapass
- Access PassView
- RockXP
- Magical Jelly Bean Keyfinder
- PstPassword
- Protected Storage PassView
- Network Password Recovery
- Mail PassView
- Asterisk Key
- Messenger Key
- MessenPass
- Password Spectator
- SniffPass
- Asterisk Logger
- Dialupass
- Mail Password Recovery
- Database Password Sleuth
- CHAOS Generator
- PicoZip Recovery
- Crack
- Brutus
- Distributed John

- Common Recommendations for Improving Password Security
- Standard Password Advice

Module 25: Log Capturing and Event Correlation

- Computer Security Logs
    - Computer Security Logs
    - Operating System Logs
    - Application Logs
    - Software Security Logs
    - Router Log Files

  - Honeypot Logs
  - Linux Process Accounting
  - Logon Event in Window
  - Windows Log File
  - Configuring Windows Logging
  - Analyzing Window Log
  - Setting up Remote Logging in Windows
  - Windows Log File: System Logs
  - Windows Log File: Application Logs
  - Log on Events That Appear in the Security Event Log
  - IIS Logs
  - Maintaining Credible IIS Log Files
  - Log File Accuracy
  - Log Everything
  - Keeping Time
  - UTC Time
  - View the DHCP Logs
  - DHCP Logs
  - ODBC Logging
- Logs and Legal Issues
  - Legality of Using Logs
  - Records of Regularly Conducted Activity as Evidence
  - Laws and Regulations
- Log Management
  - Log Management
  - Functions of Log Management
  - Challenges in Log Management
- Centralized Logging and Syslogs
  - Central Logging Design
  - Steps to Implement Central Logging
  - Syslog
  - Syslog in Unix-like Systems
  - Steps to Set Up Syslog Server for Unix Systems
  - Centralized Syslog Server
  - IIS Centralized Binary Logging
  - Extended Logging in IIS Server
- Time Synchronization

  - Why Synchronize Computer Times?
  - What is NTP Protocol?
  - NTP Stratum Levels
  - NIST Time Servers
  - Configuring the Windows Time Service
- Event Correlation
  - Event Correlation
  - Types of Event Correlation
  - Prerequisites for Event Correlation
  - Event Correlation Approaches
- Log Capturing and Analysis Tools
  - Syslog-ng Logging System
  - WinSyslog Syslog Server
  - Kiwi Syslog Server
  - Tenable Security Center
  - IISLoger: Development tool
  - Socklog: IDS Log Analysis Tool
  - Microsoft Log Parser: Forensic Analysis Tool
  - Firewall Analyzer: Log Analysis Tool
  - Adaptive Security Analyzer (ASA) Pro
  - GFI EventsManager
  - How does GFI EventsManager work?
  - Activeworx Security Center
  - Ntsyslog
  - EventReporter
  - EventLog Analyzer
  - FLAG – Forensic and Log Analysis GUI
  - Simple Event Correlator (SEC)

Module 26: Network Forensics and Investigating Logs

- Introduction to Network Forensics
- Intrusion Process
- Network Vulnerabilities
- Network Attacks
- Looking for Evidence
- Investigating Logs
  - Postmortem and Real-Time Analysis

    - Handling Logs as Evidence
    - Log File Authenticity
    - Use Signatures, Encryption and Checksums
    - Work with Copies
    - Ensure System Integrity
    - Access Control
    - Chain of Custody
    - Condensing Log File
- Log Injection Attacks
    - New Line Injection Attack
    - New Line Injection Attack Countermeasure
    - Separator Injection Attack
    - Defending Separator Injection Attack
    - Time Stamp Injection Attack
    - Defending Time Stamp Injection Attack
    - Word Wrap Abuse Attack
    - Defending Word Wrap Abuse Attack
    - HTML Injection Attack
    - Defending HTML Injection Attack
    - Terminal Injection Attack
    - Defending Terminal Injection Attack
- Other Kinds of Log File Attacks

Module 27: Investigating Network Traffic

- Network Addressing Schemes
- OSI Reference Model
- Overview of Network Protocols
- TCP/ IP Protocol
- Overview of Physical and Data-link Layer of the OSI Model
- Overview of Network and Transport Layer of the OSI Model
- Types of Network Attacks
- Why to Investigate Network Traffic?
- Evidence Gathering Via Sniffing
- Acquiring Traffic using DNS Poisoning Techniques
- Intranet DNS Spoofing (Local Network)
- Internet DNS Spoofing (Remote Network)
- Internet DNS Spoofing

- Proxy Server DNS Poisoning
- DNS Cache Poisoning
- Evidence Gathering From ARP Table
- Evidence Gathering at the Data-link Layer: DHCP Database
- Gathering Evidence by IDS
- Traffic Capturing and Analysis Tools
    - Tool: Tcpdump
    - Tool: Windump
    - Tool: NetIntercept
    - Tool: Wireshark
    - CommView
    - Softperfect Network Sniffer
    - HTTP Sniffer
    - EtherDetect Packet Sniffer
    - OmniPeek
    - Iris Network Traffic Analyzer
    - SmartSniff
    - NetSetMan Tool
    - Distinct Network Monitor
    - Maa Tec Network Analyzer
    - Ntop
    - Etherape
    - Colasoft Capsa Network Analyzer
    - Colasoft EtherLook
    - AnalogX Packetmon
    - BillSniff
    - IE HTTP Analyzer
    - EtherDetect Packet Sniffer
    - EtherScan Analyzer
    - Sniphere
    - IP Sniffer
    - AW Ports Traffic Analyzer
    - Ipgrab
    - Nagios
    - Give Me Too
    - Sniff - O – Matic
    - EtherSnoop

- GPRS Network Sniffer: Nokia LIG
- Siemens Monitoring Center
- NetWitness
- Netresident Tool
- nGenius InfiniStream
- eTrust Network Forensics
- ProDiscover Investigator
- P2 Enterprise Shuttle (P2EES)
- Show Traffic
- Network Probe
- Snort Intrusion Detection System
- Snort IDS Placement
- IDS Policy Manager

- Documenting the Evidence Gathered on a Network
- Evidence Reconstruction for Investigation

Module 28: Router Forensics

- What is a Router?
- Functions of a Router
- A Router in an OSI Model
- Routing Table and its Components
- Router Architecture
- Routing Information Protocol
- Implications of a Router Attack
- Routers Vulnerabilities
- Types of Router Attacks
  - Router Attack Topology
  - Denial of Service (DoS) Attacks
  - Packet “Mistreating” Attacks
  - Routing Table Poisoning
  - Hit-and-Run and Persistent Attacks
- Router Forensics vs. Traditional Forensics
- Steps for Investigating Router Attacks
  - Seize the Router and Maintain Chain of Custody
- Sample Chain Of Custody (COC) Form
- Guidelines for the Router Forensic
- Incident Response

- Recording your Session
- Accessing the Router
- Volatile Evidence
- Obtaining Configuration of Router
- Volatile Evidence Gathering
- Direct Access: Using show commands
- Indirect Access: Using Scanning Tool
- Compare the Configuration of Router
- Examine the Router Table
- Examine the Access Control List
- Router Logs
- Example of Router Logs
- NETGEAR Router Logs
- Link Logger
- Sawmill: Linksys Router Log Analyzer
- Logging
- Handling a Direct Compromise Incident
- Other Incidents
- Real Time Forensics
- Router Audit Tool (RAT)
- Generate the Report

Module 29: Investigating Wireless Attacks

- Wireless Networking Technologies
- Wireless Networks
- Wireless Attacks
- Passive Attack
- Threats from Electronic Emanations
- Active Attacks on Wireless Networks
- Denial-of-Service Attacks
- Man-in-the-Middle Attack (MITM)
- Hijacking and Modifying a Wireless Network
- Association of Wireless AP and Device
- Network Forensics in a Wireless Environment
- Steps for Investigation
- Key Points to Remember
- Points You Should not Overlook while Investigating the Wireless Network

- Obtain a Search Warrant
- Document the Scene and Maintain Chain Of Custody
- Identify Wireless Devices
- Wireless Components
- Search for Additional Devices
- Detect Wireless Connections
- Detect Wireless Enabled Computers
- Manual Detection of Wireless APs
- Active Wireless Scanning Technique
- Passive Wireless Scanning Technique
- Detect WAPs using the Nessus Vulnerability Scanner
- Capture Wireless Traffic
- Tool: Wireshark
    - Feature of Wireshark
- Tool: tcpdump
    - tcpdump Commands
- ClassicStumbler
- Wireless Network Monitoring Tools
    - MacStumbler
    - iStumbler
    - AirPort Signal
    - AirFart
    - Kismet
- Determine Wireless Field Strength: Field Strength Meters (FSM)
- Prepare Wireless Zones & Hotspots Maps
- Methods to Access a Wireless Access Point
- Direct-connect to the Wireless Access Point
- Nmap
    - Scanning Wireless Access Points using Nmap
- Rogue Access Point
    - Tools to Detect Rogue Access Points: Netstumbler
    - Tools to Detect Rogue Access Points: MiniStumbler
- 2. “Sniffing” Traffic Between the Access Point and Associated Devices
- Scanning using Airodump
- MAC Address Information
- Airodump: Points to Note
- Forcing Associated Devices to Reconnect

- Check for MAC Filtering
- Changing the MAC Address
- Wireless Data Acquisition and Analysis
- Report Generation

Module 30: Investigating Web Attacks

- Indications of a Web Attack
- Types of Web Attacks
- Cross-Site Scripting (XSS)
- Investigating Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Anatomy of CSRF Attack
- Pen-Testing CSRF Validation Fields
- SQL Injection Attacks
- Investigating SQL Injection Attacks
- News: SQL Injection Attacks Against Databases Rise Sharply
- Code Injection Attack
- Investigating Code Injection Attack
- Parameter Tampering
- Cookie Poisoning
- Investigating Cookie Poisoning Attack
- Buffer Overflow/Cookie Snooping
- Detecting Buffer Overflow
- DMZ Protocol Attack/ Zero Day Attack
- Authentication Hijacking
- Investigating Authentication Hijacking
- Log Tampering
- Directory Traversal
- Cryptographic Interception
- URL Interpretation and Impersonation Attack
- Overview of Web Logs
- Investigating Web Attack
- Example of FTP Compromise
- Investigating FTP Logs
- Investigating FTP Servers
- Investigating IIS Logs
- Investigating Apache Logs

- Investigating Web Attacks in Windows-based Servers
- Web Page Defacement
- Defacement Using DNS Compromise
- Investigating DNS Poisoning
- Intrusion Detection
- Security Strategies to Web Applications
- Investigating Static and Dynamic IP Address
- Checklist for Web Security
- Statistics 2005-2007
- Statistics 2000-2007
- Dotdefender
- AccessDiver
- Log Analyzer: Server Log Analysis
- Web Attack Investigation Tools
  - Analog
  - Deep Log Analyzer
  - AWStats
  - WebLog Expert
  - AlterWind Log Analyzer
  - Webalizer
  - eWebLog Analyzer
  - N-Stealth
  - Acunetix
  - Falcove
  - AppScan
  - Watchfire AppScan
  - Emsa Web Monitor
  - WebWatchBot
  - Paros
  - HP WebInspect
  - KeepNI
  - Wikto
  - Mapper
  - N-Stalker
  - Scrawlr
  - Exploit-Me
- Tools for Locating IP Address

  - Hide Real IP
  - Whatismyip
  - IP Detective Suite
  - Enterprise IP - Address Manager
  - Whois Lookup
  - SmartWhois
  - ActiveWhois
  - LanWhois
- Nslookup
- Traceroute
- Tools for Locating IP Address
  - NeoTrace (Now McAfee Visual Trace)
  - Whois
  - CountryWhois
  - IP2Country
  - CallerIP
  - Whois.net
  - Pandora FMS
- CounterStorm-1: Defense Against Known, Zero Day, and Targeted Attacks

Module 31: Investigating DoS Attacks

- DoS Attack
- Indications of a DoS/DDoS Attack
- Types of DoS Attacks
- Ping of Death Attack
- Teardrop Attack
- SYN Flooding
- Land
- Smurf
- Fraggle and Snork Attack
- WINDOWS OUT-OF-BAND (OOB) Attack and Buffer Overflow
- Nuke Attacks and Reflected Attack
- DDoS Attack
- Working of DDoS Attacks
- Classification of DDoS Attack
- DDoS Attack Taxonomy
- DoS Attack Modes

- Techniques to Detect DoS Attack
- Techniques to Detect DoS Attack: Activity Profiling
- Techniques to Detect DoS Attack: Sequential Change-Point Detection
- Techniques to Detect DoS Attack: Wavelet-based Signal Analysis
- Monitoring CPU Utilization to Detect DoS Attacks
- Detecting DoS Attacks Using Cisco NetFlow
- Detecting DoS Attacks Using Network Intrusion Detection System (NIDS)
- Investigating DoS Attack
- ICMP Traceback
- Hop-by Hop IP Traceback
- Limitations of Hop-by Hop IP Traceback
- Backscatter Traceback
- How the Backscatter Traceback Works
- IP Traceback with IPSec
- CenterTrack Method
- Packet Marking
- Probabilistic Packet Marking (PPM)
- Check Domain Name System (DNS) Logs
- Tracing with "log-input"
- Control Channel Detection
- Correlation and Integration
- Path Identification (Pi) Method
- Packet Traffic Monitoring Tools
- Tools for Locating IP Address
- Challenges in Investigating DoS Attack
- Network Monitoring Tools
  - Nmap
  - Friendly Pinger
  - IPHost Network Monitor
  - Tail4Win
  - Status2k
  - DoSHTTP
  - Admin’s Server Monitor

Module 32: Investigating virus, Trojan, spyware and Rootkit Attacks

- Statistics of the Malicious and Potentially Unwanted Programs
- Viruses and Worms

- Virus Top 20 for January 2008
- Viruses
- Worms
- How to Know a Virus Infected a System
- Characteristics of a Virus
- Working of a Virus
  - Working of a Virus: Infection Phase
  - Working of a Virus: Attack Phase
- Symptoms of a Virus-Like Attack
- Indications of a Virus Attack
- Modes of Virus Infection
- Stages of Virus Life
- Virus Classification
- How Does a Virus Infect?
- Storage Patterns of a Virus
- Virus Detection
- Virus Detection Methods
- Virus Incident Response
- Investigating Viruses

- Trojans and Spyware
  - Trojans and Spyware
  - Working of Trojans
  - How Spyware Affects a System
  - What Spyware Does to the System
  - What Do Trojan Creators Look For?
  - Different Ways a Trojan Can Get into a System
  - Identification of a Trojan Attack
  - Remote Access Trojans (RAT)
  - Ports Used by Trojans
- Anti virus Tools
  - AVG Antivirus
  - Norton Antivirus
  - McAfee
  - Kaspersky Anti-Virus
  - BitDefender
  - SocketShield
  - CA Anti-Virus

  - F-Secure Anti-Virus
  - F-Prot Antivirus
  - Panda Antivirus Platinum
  - avast! Virus Cleaner
  - Norman Virus Control
  - ClamWin
- Anti Trojan Tools
  - TrojanHunter
  - Comodo BOClean
  - Trojan Remover: XoftspySE
  - Trojan Remover: Spyware Doctor
  - SPYWAREfighter
  - Evading Anti-Virus Techniques
  - Sample Code for Trojan Client/Server
- Evading Anti-Trojan/Anti-Virus Using Stealth Tools
- Backdoor Countermeasures
- Tool: Tripwire
- System File Verification
- MD5sum.exe
- Tool: Microsoft Windows Defender
- Rootkit
  - Introduction of Rootkit
  - Attacks Approach
  - Types of Rootkits
  - Rootkit Detection
- Windows Rootkit
  - Fu Rootkit
  - Vanquish
  - AFX Rootkit
- Linux Rootkit
  - Knark
  - Adore
  - Ramen
  - Beastkit
- Rootkit Detection Tools
  - UnHackMe
  - UnHackMe Procedure

  - F-Secure BlackLight
  - RootkitRevealer
  - Microsoft Windows Malicious Software Removal Tool
  - Rkhunter
  - chkrootkit
  - IceSword

Module 33: Investigating Internet Crimes

- Internet Crimes
- Internet Forensics
- Why Internet Forensics
- Goals of Investigation
- Investigating Internet Crime Steps
- Obtain a Search Warrant
- Interview the Victim
- Prepare Bit-Stream Copies
- Check the Logs
- Identify the Source of the Attack
- IP Address
- Internet Assigned Numbers Authority
- Regional Internet Registry (RIR)
- Internet Service Provider
- Trace the IP Address of the Attacker Computer
- Domain Name System (DNS)
- DNS Record Manipulation
- DNS Lookup
  - Nslookup
- Analyze the Whois Information
  - Whois
  - Example Whois Record
- Whois Tools and Utilities
  - Samspade
  - SamSpade Report
  - IP Address Locator
  - www.centralops.net: Tracing Geographical Location of a URL
  - DNS Lookup Result: centralops.net

  - Traceroute
- Collect the Evidence
- Examining Information in Cookies
- Viewing Cookies in Firefox
  - Tool: Cookie Viewer
- Switch URL Redirection
- Sample Javascript for Page-based Redirection
- Embedded JavaScript
- Downloading a Single Page or an Entire Web Site
  - Tool: My Offline Browser
- Recovering Information from Web Pages
  - Tool: WayBack Machine
  - *Take Me Back* Results
- Investigation Tool
  - Grab-a-Site
  - SurfOffline
  - Trace the Email
  - https://www.abika.com/forms/Verifyemailaddress.asp
- HTTP Headers
- Email Headers Forging
- Viewing Header Information
- Tracing Back Spam Mails
  - VisualRoute
  - NeoTrace (Now McAfee Visual Trace)
  - NetScanTools Pro
- Report Generation

Module 34: Tracking Emails and Investigating Email crimes

- Email System
- E-mail Client
- E-mail Server
- SMTP Server
- POP3 and IMAP Server
- Importance of Electronic Records Management
- E-mail Crime
- Spamming
- Mail Bombing/Mail Storm

- Crime via Chat Rooms
- Identity Fraud/Chain Letter
- Phishing
- Email Spoofing
- Investigating E-mail Crime and Violation
- Obtain a Search Warrant and Seize the Computer and Email Account
- Obtain a Bit-by-Bit Image of Email Information
- Email Message
- Viewing Header in Microsoft Outlook
- Viewing Header in AOL
- Viewing Headers in Hotmail
- Viewing Header in Gmail
- Viewing Header in Yahoo Mail
- Examining an Email Header
- Analysis of Email Header at Timmy
- Received: Headers
- Forging Headers
- List of Common Headers
- Examining Additional Files (.pst or .ost files)
    - Pst File Location
- Microsoft Outlook Mail
- Examine the Originating IP Address
- http://centralops.net/co/
- Exchange Message Tracking Center
- MailDetective Tool
- Examine Phishing
- Forensic ToolKit (FTK)
- E-Mail Examiner by Paraben
- Network E-Mail Examiner by Paraben
- Recover My Email for Outlook
- Diskinternals – Outlook Recovery
- Tracing Back
- Tracing Back Web Based E-mail
- Abuse.Net
- Network Abuse Clearing House
- Tool: LoPe
- Tool:FINALeMAIL

- Handling Spam
- Tool: eMailTrackerPro
- Email Trace
- Tool: ID Protect
- Email Investigation Tool
    - R-Mail
    - Email Detective
    - SPAM Punisher
    - SpamArrest
- U.S. Laws Against Email Crime: CAN-SPAM Act
- U.S.C. § 2252A
- U.S.C. § 2252B
- Email Crime Law in Washington: RCW 19.190.020

Module 35: PDA Forensics

- Personal Digital Assistant (PDA)
- Information Stored in PDA
- PDA Components
- PDA Characteristics
- Generic PDA Hardware Diagram
- Palm OS
- Architecture of Palm OS Devices
- Pocket PC
- Architecture for Windows Mobile
- Linux-based PDAs
- Architecture of the Linux OS for PDAs
- PDA Generic States
- PDA Security Issues
- ActiveSync and HotSync Features
- ActiveSync Attacks
- HotSync Attacks
- PDA Fornnsics
    - PDA Forensics steps
    - Points to Remember while Conducting Investigation
    - Securing and Evaluating the Scene
    - Seize the Evidences
    - Identify the Evidence

    - Preserve the Evidence
    - Acquire the Information
    - Data Acquisition Techniques
    - Examination and Analysis the Information
    - Document Everything
    - Make the Report
- PDA Forensic Tool
    - PDA Secure
    - Device Seizure
    - DS Lite
    - EnCase
    - SIM Card Seizure
    - Palm dd (pdd)
    - Duplicate Disk
    - Pocket PC Forensic Software
    - Mobile Phone Inspector
    - Memory Card Data Recovery Software
- PDA Security Countermeasures

Module 36: Blackberry Forensics

- Blackberry
- BlackBerry Operating System
- How BlackBerry Works
- BlackBerry Serial Protocol
- BlackBerry Serial Protocol: Packet Structure
- Blackberry Attack
- Blackberry Attack Toolkit
- BlackBerry Attachment Service Vulnerability
- TeamOn Import Object ActiveX Control vulnerability
- Denial of Service in BlackBerry Browser
- BlackBerry Security
- BlackBerry Wireless Security
- BlackBerry Security for Wireless Data
- Prerequisites for BlackBerry Forensics
- Steps for BlackBerry Forensics
- Collect the Evidence
- Document the Scene and Preserve the Evidence

- Radio Control
- Imaging and Profiling in BlackBerry
- Acquire the Information
- Hidden Data in BlackBerry
- Acquire Logs Information from BlackBerry
- Program Loader
- Review of Information
- Best Practices for Protecting Stored Data
- BlackBerry Signing Authority Tool
- Forensics Tool: RIM BlackBerry Physical Plug-in
- ABC Amber BlackBerry Converter
- Packet PC
- ABC Amber vCard Converter
- BlackBerry Database Viewer Plus

Module 37: iPod and iPhone Forensics

- iPod
- iPhone Overview
- What a Criminal Can do With iPod
- What a Criminal Can do With iPhone
- iPhone OS Overview
- iPhone Disk Partitions
- Apple HFS+ and FAT32
- Application Formats
- iPod and iPhone Forensics
- Evidence Stored on iPod and iPhone
- Forensic Prerequisites
- Collecting iPod/iPhone Connected with Mac
- Collecting iPod/iPhone Connected with Windows
- Disable Automatic Syncing
- Write Blocking
- Write Blocking in Different OS
- Image the Evidence
- View the iPod System Partition
- View the Data Partition
- Break Passcode to Access the Locked iPhone
- Acquire DeviceInfo File

- Acquire SysInfo File
- Recover IPSW File
- Check the Internet Connection Status
- View Firmware Version
- Recover Network Information
- Recovering Data from SIM Card
- Acquire the User Account Information
- View the Calendar and Contact Entries
- Recovering Photos
- Recovering Address Book Entries
- Recovering Calendar Events
- Recovering Call Logs
- Recovering Map Tile Images
- Recovering Cookies
- Recovering Cached and Deleted Email
- Recover Deleted Files
- Forensic Information from the Windows Registry
- Forensic Information from the Windows: setupapi.log
- Recovering SMS Messages
- Other Files Which are Downloaded to the Computer During iTunes Sync Process
- Analyze the Information
- Timeline Generation
- Timeline Generation: File Status After Initialization the iPod with iTunes and Before Closing iTunes
- Timeline Generation: File Status After Connecting iPod to the Computer for Second Time, Copying Music, and Closing iTunes
- Time Issues
- Jailbreaking in iPod Touch and iPhone
  - Jailbreaking
  - AppSnapp
  - iFuntastic
  - Pwnage: Tool to Unlock iPod Touch
  - Erica Utilities for iPod Touch
- Tools
  - EnCase
  - DiskInternals Music Recovery
  - Recover My iPod: Tool
  - iPod Data Recovery Software

  - iPod Copy Manager
  - Stellar Phoenix iPod Recovery
  - Aceso
  - Cellebrite UME 36 Pro
  - Walf
  - Device Seizure
  - PhoneView
  - iPhone Drive
  - Tansee iPhone Transfer SMS
  - SIM Analyzer
  - SIMCon – SIM Card Recovery
  - SIM Card Data Recovery Software

Module 38: Cell Phone Forensics

- Mobile Phone
- Hardware Characteristics of Mobile Devices
- Software Characteristics of Mobile Devices
- Components of Cellular Network
- Cellular Network
- Different Cellular Networks
- Different OS in Mobile Phone
- What a Criminal Can do with Mobiles
- Mobile Forensics
- Forensics Information in Mobile Phones
- Subscriber Identity Module (SIM)
- SIM File System
- Integrated Circuit Card Identification (ICCID)
- International Mobile Equipment Identifier (IMEI)
- Electronic Serial Number (ESN)
- Precaution to be Taken before Investigation
- Points to Remember while Collecting the Evidence
- Acquire the Information
- Acquire Data from SIM Cards
- Acquire Data from Unobstructed Mobile Devices
- Acquire the Data from Obstructed Mobile Devices
- Memory Considerations in Mobiles
- Acquire Data from Memory Cards

- Memory Cards
- Acquire Data from Synched Devices
- Gather Data from Network Operator
- Check Call Data Records (CDR's)
- Analyze the Information
- Cell Phone Forensic Tools
  - SIM Analyzer
  - SIMCon
  - SIM Card Data Recovery
  - Memory Card Data Recovery
  - Device Seizure
  - SIM Card Seizure
  - Cell Phone Analyzer
  - Oxygen Forensic Suite
  - BitPim
  - MOBILedit! Forensic
  - PhoneBase
  - Secure View
  - XACT
  - CellDEK
    Forensic Card Reader (FCR)
  - ForensicSIM Toolkit
  - SIMIS 3G
  - UME-36Pro - Universal Memory Exchanger
  - Cellebrite UFED System - Universal Forensic Extraction Device
  - ZRT
  - Neutrino
  - ICD 5005
  - ICD 1300
- Challenges for Forensic Efforts

Module 39: USB Forensics

- Universal Serial Bus (USB)
- USB Flash Drive
- Screenshot: USB Flash Drive
- Misuse of USB
- USB Forensics

- USB Forensic Investigation
- Secure and Evaluate the Scene
- Document the Scene and Devices
- Image the Computer and USB Device
- Acquire the Data
- Check Open USB Ports
- Examine Registry of Computer: USBTOR
- Examine Registry of Computer: DeviceClasses
- Examine Registry of Computer: MountedDevice
- Generate Reports
- USB Forensic Tools
  - Bad Copy Pro
  - Data Doctor Recovery
  - USB Image Tool
  - USBDeview

Module 40: Printer Forensics

- Introduction to Printer Forensics
- Different Printing Modes
- Methods of Image Creation
- Printers with Toner Levels
- Parts of a Printer
- Printer Identification Strategy
  - Printer Identification
- Printer Forensics Process
  - Pre-Processing
  - Printer Profile
  - Forensics
  - Ballistics
- A Clustering Result of a Printed Page
- Digital Image Analysis
- Printout Bins
- Document Examination
  - Services of Document Examiner
  - Tamper-proofing of Electronic and Printed Text Documents
- Phidelity
- Zebra Printer Labels to Fight against Crime

- Cryptoglyph Digital Security Solution
- Case Study
- Is Your Printer Spying On You?
- DocuColor Tracking Dot Decoding
- Tools
  - Print Spooler Software
  - Investigating Print Spooler
  - iDetector
  - Print Inspector
  - EpsonNet Job Tracker

Module 41: Investigating Corporate Espionage

- Investigating Corporate Espionage: Case Study
- Introduction to Corporate Espionage
- Motives Behind Spying
- Information that Corporate Spies Seek
- Corporate Espionage: Insider/Outsider Threat
- Threat of Corporate Espionage due to Aggregation of Information
- Techniques of Spying
- Defense Against Corporate Spying
- Controlled Access
- Background Investigation of the Personnel
- Basic Security Measures to Protect Against Corporate Spying
- Steps to Prevent Corporate Espionage
- Key Findings from U.S Secret Service and CERT Coordination Center/SEI study on Insider Threat
- Netspionage
- Investigating Corporate Espionage Cases
- Employee Monitoring: Activity Monitor
- Spector CNE Employee Monitoring Software
- Track4Win
- Spy Tool
  - SpyBuddy
  - NetVizor
  - Privatefirewall w/Pest Patrol
- Anti Spy Tool
  - Internet Spy Filter
  - Spybot S&D

    - SpyCop
    - Spyware Terminator
    - XoftSpySE
- Spy Sweeper
- Counter Spy
- SUPERAntiSpyware Professional
- IMonitorPCPro - Employee Monitoring Software
- Case Study: HP Chief Accused of Corporate Spying
- Case Study: India's Growing Corporate Spy Threat
- Guidelines while Writing Employee Monitoring Policies

Module 42: Investigating Computer Data Breaches

- How Data Breaches Occur
    - Using The External Memory Devices
    - Using The Internet
    - Using Mobiles And iPods
    - Using Malware
    - Others Techniques
- Investigating Local Machine
    - Check The Registry Editor
    - Check For CD/DVD Burning Software
    - Check For Browsing History
    - Check The Downloads
    - Check The Mail History
    - Check For Suspicious Software
- Investigating Network
    - Check The Firewall
    - Check The Mail Server
    - Check The Printers
- Countermeasures

Module 43: Investigating Trademark and Copyright Infringement

- Trademark Infringement
    - Trademarks
    - Trademark Eligibility and Benefits of Registering It
    - Service Marks and Trade Dress
    - Trademark Infringement

  - Monitoring Trademark Infringements
  - Key Considerations before Investigating Trademark Infringements
  - Steps for Investigating Trademark Infringements
- Copyright Infringement
  - Copyright
  - Investigating Copyright Status
  - How Long Does a Copyright Last?
  - U.S Copyright Office
  - How is Copyrights Enforced?
  - Copyright Infringement: Plagiarism
  - Types of plagiarism
  - Steps for Plagiarism Prevention
  - Plagiarism Detection Factors
- Plagiarism Detection Tools
  - Turnitin
  - CopyCatch
  - Copy Protection System (COPS)
  - SCAM (Stanford Copy Analysis Mechanism)
  - CHECK
  - Jplag
  - VAST
  - SIM
  - Urkund
  - WCopyfind
  - GPSP
  - PLAGUE
  - SPlaT
  - Sherlock
  - PRAISE
  - SafeAssignment
  - EVE2
  - iThenticate
  - Dupli Checker
  - http://www.plagiarismdetect.com/
  - http://www.plagiarism.org.uk/
- Patent Infringement
  - Patent

  - Patent Infringement
  - Types of Patent Infringement
  - Patent Search
  - http://www.ip.com
  - How ip.com Works
  - Domain Name Infringement
  - How to Check for Domain Name Infringement?
- Intellectual Property
  - Intellectual Property
  - Investigating Intellectual Property Theft
  - Steps for Investigating Intellectual Property Theft
- Digital Rights Management
  - Digital Rights Management (DRM)
- Windows Media Digital Rights Management
- Media-DRM Packager
- Haihaisoft Media DRM Packager
- DRM Software for Copy Protection
- IntelliProtector
- Trademarks and Copyright Laws
  - US Laws for Trademarks and Copyright
  - Indian Laws for Trademarks and Copyright
  - Japanese Laws for Trademarks and Copyright
  - Australia Laws For Trademarks and Copyright
  - UK Laws for Trademarks and Copyright
  - China Laws for Trademarks and Copyrigh
  - Canada Laws for Trademarks and Copyright
  - South African Laws for Trademarks and Copyright
  - South Korean Laws for Trademarks and Copyright
  - Belgium Laws for Trademarks and Copyright
  - Hong Kong Laws for Intellectual Property

Module 44: Investigating Sexual Harassment Incidents

- Sexual Harassment - Introduction
- Types of Sexual Harassment
- Consequences of Sexual Harassment
- Sexual Harassment Statistics
- Do’s and Don'ts if You Are Being Sexually Harassed

- Stalking
- Stalking Behaviors
- Stalking Effects
- Guidelines for Stalking Victims
- Responsibilities of Supervisors
- Responsibilities of Employees
- Complaint Procedures
  - Informal procedures
  - Formal procedures
- Investigation Process
  - Investigation Process
  - Sexual Harassment Investigations
  - Sexual Harassment Policy
  - Preventive Steps
- Laws on Sexual Harassment
  - U.S Laws on Sexual Harassment
  - The Laws on Sexual Harassment: Title VII of the 1964 Civil Rights Act
  - The Laws on Sexual Harassment: The Civil Rights Act of 1991
  - The Laws on Sexual Harassment: Equal Protection Clause of the 14th Amendment
  - The Laws on Sexual Harassment: Common Law Torts
  - The Laws on Sexual Harassment: State and Municipal Laws
  - Australian Laws on Sexual Harassment
  - The Laws on Sexual Harassment: Sex Discrimination Act 1984
  - The Laws on Sexual Harassment: Equal Opportunity for Women in the Workplace Act 1999
  - The Laws on Sexual Harassment: Anti-Discrimination Act 1991
  - The Laws on Sexual Harassment: Workplace Relations Act 1996
  - Indian Law: Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Bill, 2006
  - German Law: Protection of Employees Act
  - UK Law: The Employment Equality (Sex Discrimination) Regulations 2005
  - Law of the People's Republic of China on the Protection of Rights and Interests of Women
  - Penal Code, Section 509. in Malaysia
- Sample Complaint Form
- Laws Against Stalking

Module 45: Investigating Child Pornography Cases

- Introduction to Child Pornography

- People's Motive Behind Child Pornography
- People Involved in Child Pornography
- Role of Internet in Promoting Child Pornography
- Effects of Child Pornography on Children
- Measures to Prevent Dissemination of Child Pornography
- Challenges in Controlling Child Pornography
- Precautions before Investigating Child Pornography Cases
- Steps for Investigating Child Pornography
    - Step 1: Search and Seize all Computer and Media Devices
    - Step 2: Check Authenticated Login Sessions
    - Step 3: Search Hard Disk for Pornographic Material
    - Step 4: Recover Deleted Files and Folders
    - Step 5: Check Metadata of Files and Folders Related with Pornography
    - Step 6: Check and Recover the Browser Information
        - Browsing History, Save Form, and Search History
        - Download History
        - Cache
        - Cookies
        - Saved Passwords
        - Authenticated Sessions
    - Step 7: Check ISP Logs
- Sources of Digital Evidence
- Citizens' Responsibility on pornography
- Guidelines to Avoid Child Pornography on the Web
- Guidelines for Parents to Protect Children from Pornography
- Tools to Protect Children from Pornography
    - Reveal
    - iProtectYou
    - WUPC Web Control for Parents 4
    - BrowseControl
    - ChatGuard
    - Child Exploitation Tracking System (CETS)
- Reports on Child Pornography
- Laws Against Child Pornography
    - U.S. Laws against Child Pornography
    - Australia Laws against Child Pornography
    - Austria Laws against Child Pornography

  - Belgium Laws against Child Pornography
  - Cyprus Laws against Child Pornography
  - Japan Laws against Child Pornography
  - South African Laws against Child Pornography
  - UK laws against Child Pornography
  - State Laws: Michigan Laws against Child Pornography
  - England and Wales Laws
  - Scotland laws
  - Philippines laws (Republic Acts)
  - Children's Internet Protection Act (CIPA)
- Anti-Child-Pornography Organizations
  - Innocent Images National Initiative
  - Internet Crimes against Children (ICAC)
  - Antichildporn.org
  - How to Report to Antichildporn.org about Child Pornography Cases
  - Child Exploitation and Online Protection (CEOP) Centre
  - ThinkUKnow
  - Virtual Global Taskforce (VGT)
  - Internet Watch Foundation (IWF)
  - International Centre for Missing & Exploited Children (ICMEC)
  - National Center for Missing & Exploited Children (NCMEC)
  - Child Victim Identification Program (CVIP)
  - Financial Coalition against Child Pornography (FCACP)
  - Perverted Justice
  - National Society for the Prevention of Cruelty to Children (NSPCC)
  - Canadian Centre for Child Protection
  - http://cybertip.ca/
  - Association of Sites Advocating Child Protection (ASACP)
  - Web Sites against Child Porn (WSACP)
  - http://www.reportchildporn.com/
  - Child Focus
  - StopChildPorno.be

Module 46: Investigating Identity Theft Cases

- Identity Theft
  - Identity Theft
  - Identifying Information

- Identity Theft Statistics for 2007
- Identity Theft Complaints By Age of The Consumer
- Example of Identity Theft
- Who Commits Identity Theft
- How Criminals Get Information
- How Personal Information Was Stolen: Statistics
- Techniques Used By Criminals
- How Does A Criminal Use Information
- FTC Consumer Sentinel
- Identity Theft Movies

- Investigating Identity Theft
    - Investigating Identity Theft
    - Interview The Victim
    - Get The Credit Reports
    - Sample Credit Report
    - Collect Information About Online Activities of Victim
    - Collect Information About The Websites Where Victim Has Disclosed Personal Information
        - http://www.whois.net/
        - http://centralops.net/co/
        - http://www.archive.org/
    - Search The FTC Consumer Sentinel
    - Collect Information From Point Of Sale
    - Collect Information From Courier Services
    - Get Call Records From Service Providers If Stolen Identity Is Used To Obtain Phone Service
    - Search The Suspect's Address
    - Obtain Search And Seize Warrant
    - Seize The Computer And Mobile Devices From Suspects
    - Collect The Browser Information From Suspects Computer
- Identity Theft Laws
    - United States: Federal Identity Theft and Assumption Deterrence Act of 1998
    - Unites States Federal Laws
    - Australia
    - Canada
    - Hong Kong
    - United Kingdom
- Protection From Identity Theft
    - Protection From ID Theft

- What Should Victims Do?
- Resources for Victims

Module 47: Investigating Defamation over Websites and Blog Postings

- What is a Blog
- Types of Blogs
- Blogging
- Who is Blogging?
- Blogosphere Growth
- Defamation over Websites and Blog Postings
- Steps for Investigating Defamation Over Websites and Blog Postings
- Search the Content of Blog in Google
- Check the URL of the Blog/Webpage
- Check the Copyright and Privacy Policy
- Check the Profile of Author of the Blog/Web Post
- Intelius Search (www.intelius.com)
- Yahoo! People Search
- Satellite Picture of a Residence
- Best PeopleSearch (http://www.bestpeoplesearch.com/)
- People-Search-America.com
- Check the Comments for the Blog
- Search in www.archive.org
- Search Results
- Check in Whois Database
- Whois Database Result
- Search the Email Address and Telephone Number
- Visit 411 and Search for Telephone Numbers
- Search for UK Telephone Numbers at BT
- Check the Physical Location

Module 48: Investigating Social Networking Websites for Evidences

- Introduction: Social Networking
- What Is a Social Networking Site
- MySpace
- Facebook
- Orkut
- Crime Using Social Networking Website

- Use of Social Networking Websites in Investigations
- Investigation Process
- Search for Convict Account on Website
- Mirror the web pages in the CD-ROM
- Investigation in MySpace
- Investigation in Facebook
- Investigation in Orkut
- Investigating Profile
- Investigating Scrapbook
- Investigating Photos and Video
- Investigating Testimonials
- Investigating View Events
- Investigating Friendlist
- Investigating Communities
- Report Generation

Module 49: Investigation Search Keywords

- Keyword Search
- Developing a Keyword Search List
- Index-Based Keyword Searching
- Bitwise Searching
- Keyword Search Techniques
- Choice of Searching Methodology
- Issues with Keyword Searching
- Odyssey Keyword Search

Module 50: Investigative Reports

- Computer Forensic Report
- Computer Forensic Rreport Template
- Report Specifications
- Report Classification
- Layout of an Investigative Report
- Guidelines for Writing a Report
- Use of Supporting Material
- Importance of Consistency
- Salient Features of a Good Report
- Important Aspects of a Good Report

- Investigative Report Format
- Attachments and Appendices
- Include Metadata
- Signature Analysis
- Sample Forensic Report
- Investigation Procedures
- Collecting Physical and Demonstrative Evidence
- Collecting Testimonial Evidence
- Dos and Don'ts of Forensic Computer Investigations
- Case Report Writing and Documentation
- Create a Report to Attach to the Media Analysis Worksheet
- Best Practices for Investigators
- Writing Report Using FTK

Module 51: Becoming an Expert Witness

- What is an Expert Witness
- Role of an Expert Witness
- What Makes a Good Expert Witness?
- Types of Expert Witnesses
    - Computer Forensics Experts
    - Role of Computer Forensics Expert
    - Medical & Psychological Experts
    - Civil Litigation Experts
    - Construction & Architecture Experts
    - Criminal Litigation Experts
- Scope of Expert Witness Testimony
- Technical Testimony vs. Expert Testimony
- Preparing for Testimony
- Evidence Preparation and Documentation
- Evidence Processing Steps
- Checklists for Processing Evidence
- Examining Computer Evidence
- Prepare the Report
- Evidence Presentation
- Rules Pertaining to an Expert Witness’ Qualification
- Daubert Standard
- Frye Standard

- Importance of Resume
- Testifying in the Court
- The Order of Trial Proceedings
- General Ethics while Testifying
- Importance of Graphics in a Testimony
- Helping your Attorney
- Avoiding Testimony Issues
- Testifying during Direct Examination
- Testifying during Cross Examination
- Deposing
- Recognizing Deposing Problems
- Guidelines to Testify at a Deposing
- Dealing with Media
- Finding an Computer Forensic Expert

Module 52: How to Become a Digital Detective

- Digital Detective
- Roles and Responsibilities of Digital Detectives
- Traits of a Digital Detective
- Technical Skills
- Qualification of Digital Detectives
- Wider Competencies
- Computer Forensics Training and Certification
- Join Online Forums
- Knowledge About Law

Module 53: Computer Forensics for Lawyers

- Computer Forensics for Lawyers
- Initial Information to be Known by Lawyers When an Incident Occurs
- Presenting the Case
- What Lawyers Should Know
- Functions of Lawyers
- When Do Lawyers Really Need to Hire a Forensic Expert?
- Identify the Right Forensic Expert
- Industry Associations Providing Expert Forensic Investigators
- Check for Legitimacy

- What Lawyers Should Know in the Forensic Process
- What Makes Evidence Inadmissible in the Court
- Computer Forensics Cases
- What Lawyers Should Expect from Forensic Examiner

Module 54: Law and Computer Forensics

- Computer Forensics Laws
- Role of Law Enforcement Agencies in Forensics Investigation
- Guidelines for Law Enforcement Agencies
- Law Enforcement Policies
- Internet Laws and Statutes
  - Federal Laws (Computer Crime)
  - Intellectual Property Rights
  - Cyber Stalking
- Information Security Acts
  - The USA Patriot Act of 2001
  - Federal Information Security Management Act
  - Gramm-Leach Bliley Act
  - CAN-SPAM Act
  - Personal Information Protection and Electronic Documents Act
  - Data Protection Act 1998
  - Criminal Damage Act 1991
  - Cyber Terrorism Preparedness Act of 2002
- Laws Related to Information Assurance and Security
  - Federal Records Act
  - Federal Managers Financial Integrity Act of 1982
  - Federal Property and Administration Service Act
  - Government Paperwork Elimination Act
  - Paperwork Reduction Act
  - Computer Fraud and Abuse Act
  - Freedom of Information Act
  - E-Government Act 0f 2002 /Public Law 107-347
  - Implications of Public Law 107-347 Regarding Certification and Accreditation
  - Information Privacy Act 2000
  - National Archives and Records Act
- Computer Crime Acts
  - Australia: The Cybercrime Act 2001

  - Austrian Laws
  - Belgium Laws
  - Brazilian Laws
  - Canadian Laws
  - Denmark Laws
  - European Laws
  - France Laws
  - German Laws
  - Greece Laws
  - Hongkong Laws
  - Indian Laws
  - Italian Laws
  - Japanese Laws
  - Latvian Laws
  - Malaysian Laws
  - Malta laws
  - Netherlands Laws
  - Norwegian Laws
  - Philippines Laws: Electronic Commerce Act of 2000
  - Singapore Laws: Computer Misuse Act
  - United Kingdom: Police and Justice Act 2006
  - United States Laws
- Internet Crime Schemes and Prevention Tips
  - Internet Crime Schemes
  - Internet Crime Prevention Tips
- Reporting a Cybercrime
  - Why You Should Report Cybercrime
  - Reporting Computer-related Crimes
    - Person Assigned to Report the Crime
    - When and How to Report an Incident?
    - Who to Contact at the Law Enforcement?
    - Federal Local Agents Contact
      - More Contacts
  - CIO Cyberthreat Report Form
- Crime Investigating Organizations
  - Crime Investigating Organizations
  - Interpol - Information Technology Crime Center

  - *www.interpol.int*
  - Federal Bureau of Investigation
  - How the FBI Investigates Computer Crime
  - Federal Statutes Investigated by the FBI
  - Contact FBI Form
  - National White Collar Crime Center (NW3C)
  - Internet Crime Complaint Center (IC3)
  - Department of Homeland Security
  - National Infrastructure Protection Center
  - The G8 Countries: Principles to Combat High-tech Crime
  - The G8 Countries: Action Plan to Combat High-Tech Crime (International Aspects of Computer Crime)
  - Crime Legislation of EU
  - Law Enforcement Interfaces (EnRoute)

Module 55: Computer Forensics and Legal Compliance

- Legal Compliance
  - Regulatory Compliance and Computer Forensics
  - Legal and Liability Issues
  - Information Security Compliance Assessment
- Legal Compliance Program
  - Principles of Legal Compliance Program
  - Elements of an Effective Compliance Program
  - Role of Senior Management in Compliance Program
  - Importance of Compliance and Ethics Programs
  - Benefits of Compliance Program
  - Best Practices for Successful Implementation of a Compliance Program
  - Compliance Program Checklist
  - Compliance with Consent Decrees
  - Memoranda of Understanding/ Agreement (MOU/MOA)
  - Enterprise Compliance and Risk Analysis
  - Creating Effective Compliance Training Program
  - Responsibilities of Senior Systems Managers
  - Legal Compliance to Prevent Fraud, Waste, and Abuse
- Terms Related to Legal Compliance
  - Copyright Protection
  - Copyright Licensing

  - Criminal Prosecution
  - Due Diligence
  - Evidence Collection and Preservation
  - Importance of Evidence Collection
  - Importance of Evidence Preservation

Module 56: Security Policies

- Access Control Policy
- Administrative Security Policies and Procedures
- Audit Trails and Logging Policies
- Documentation Policy
- Evidence Collection and Preservation Policies
- Information Security Policy
- National Information Assurance (IA) Certification & Accreditation (C&A) Process Policy
- Personnel Security Policies & Guidance

Module 57: Risk Assessment

- Risk
- Security Planning
- Risk Management
  - Importance of Risk Management
- Principle of Risk Management
- IT Security Risk Management
- Risk Analysis
- Conduct Business Impact Analysis (BIA)
- Roles and Responsibilities of all the Players in the Risk Analysis Process
- Risk Analysis and/or Vulnerability Assessment Components
- Risk Policy
- Risk Assessment
  - Importance of Risk Assessment
- Approval to Operate (ATO) and Interim Approval to Operate (IATO)
  - Importance of Risk Assessment to Obtain an IATO and ATO
- Risk Assessment Methodology
- Information Sources for Risk Assessments
- Risk Assessment Process
  - Develop Policy and Procedures for Conducting a Risk Assessment
  - Write Risk Assessment Reports

    - Coordinate Resources to Perform a Risk Assessment
    - Risk Assessment Plan
- Analyze Threats and Vulnerabilities of an Information System
- Residual Risk
    - Explain Residual Risk
- Residual Risk Policy
    - Residual Risk Standard: ISO/IEC 27005:2008
- Cost/benefit Analysis
    - Cost/Benefit Analysis for Information Assurance
- Importance of Cost/Benefit Analysis for Information Assurance
- Cost/benefit Analysis Procedure
- Risk Acceptance
    - Risk Acceptance Process
- Management's Risk Acceptance Posture
- Risk Assessment and Countermeasures
- Risk Analysts
- Risk Mitigation
- Risk and Certification/Accredition of Information Systems
    - Role of Systems Certifiers and Accreditors in Risk Mitigation
- Role of Documentation in Reducing Risk

Module 58: Evaluation and Certification of Information Systems

- Accreditation
    - Importance of Accreditation
    - Types of Accreditation
    - Site Accreditation
    - Significance of NSTISSP
- Approval to Operate (ATO)
- Interim Approval to Operate (IATO)
    - Systems Security Authorization Agreement (SSAA)
        - Contents of SSAA
    - Justification for Waiver
- Cost-Benefit Analysis
- Information Classification
- Importance of Information Classification
- Investigative Authorities
- Key Management Infrastructure

- Information Marking
- Certification Test & Evaluation (CT&E)
- Certification Tools
- Product Assurance
  - Protection Profiles
  - Security Targets
- Contracting For Security Services
- Disposition of Classified Material
- Optical Remanence
- Magnetic Remanence
- Facilities Planning
  - Importance of Facilities Planning
- System Disposition/Reutilization
- Life Cycle System Security Planning
- System Security Architecture
- C&A Process for Information System
- C&A Life Cycle
  - Responsibilities Associated with Accreditation
  - Roles Associated with Certification
- Information Ownership

Module 59: Ethics in Computer Forensics

- Introduction to Computer Forensic Ethics
- Procedure to Implement Ethics
- Importance of Computer Ethics
- Challenges in Teaching Computer Forensics Ethics
- Ethical Predicaments
- The Ethical Requirements During Investigation
- Ethics in Preparation of Forensic Equipments
- Ethics of Computer Forensic Investigator
- Maintaining Professional Conduct
- Ethics in Logical Security
- Ethics in Obtaining the Evidence
- Ethics while Preserving the Evidence
- Ethics in Documenting Evidence
- Ethics in Bringing Evidence to Courtroom

Module 60: Computer Forensic Tools

- Software Forensic Tools
  - Visual TimeAnalyzer
  - X-Ways Forensics
  - Evidor
  - Slack Space & Data Recovery Tools:
  - Ontrack
  - Data Recovery Tools:
    - Device Seizure 1.0
    - Data Recovery Tools: Forensic Sorter v2.0.1
    - Data Recovery Tools: Directory Snoop
  - Permanent Deletion of Files:
    - PDWipe
    - Permanent Deletion of Files: Darik's Boot and Nuke (DBAN)
  - File Integrity Checker:
    - FileMon
    - File Date Time Extractor (FDTE)
    - Decode - Forensic Date/Time Decoder
  - Disk Imaging Tools: Snapback Datarrest
  - Partition Managers: Partimage
  - Linux/Unix Tools: Ltools and Mtools
  - Password Recovery Tool:
    - @Stake
    - Password Recovery Tool: Decryption Collection Enterprise
    - Password Recovery Tool: AIM Password Decoder
    - Password Recovery Tool: MS Access Database Password Decoder
  - Internet History Viewer:
    - CookieView - Cookie Decoder
      - Internet History Viewer: Cookie Viewer
      - Internet History Viewer: Cache View
      - Internet History Viewer: FavURLView - Favourite Viewer
      - Internet History Viewer: NetAnalysis
  - Multipurpose Tools:
    - Maresware
    - Multipurpose Tools: LC Technologies Software
    - Multipurpose Tools: Winhex Specialist Edition

- Multipurpose Tools: Prodiscover DFT

- Toolkits:
  - NTI Tools
  - Toolkits: R-Tools-I
  - Toolkits: R-Tools-II
  - Toolkits: Datalifter
  - Toolkits: Accessdata
  - FTK – Forensic Toolkit
  - Toolkit: Fastbloc
  - Toolkit: Encase
- Email Recovery Tool:
  - E-mail Examiner
  - Network E-mail Examiner
- Case Agent Companion
- Chat Examiner
- Forensic Replicator
- Registry Analyzer
- ASR Data's SMART
- Oxygen Phone Manager
- SIM Card Seizure
- Text Searcher
- Autoruns
- Autostart Viewer
- Belkasoft RemovEx
- HashDig
- Inforenz Forager
- KaZAlyser
- DiamondCS OpenPorts
- Pasco
- Patchit
- PE Explorer
- Port Explorer
- PowerGREP
- Process Explorer
- PyFLAG
- Registry Analyzing Tool: Regmon

  - Reverse Engineering Compiler
  - SafeBack
  - TapeCat
  - Vision
- Hardware Computer Forensic Tools
  - Hard Disk Write Protection Tools
    - PDBlock
    - Nowrite & Firewire Drivedock
    - LockDown
    - Write Protect Card Reader
    - Drive Lock IDE
    - Serial-ATA DriveLock Kit
    - Wipe MASSter
    - ImageMASSter Solo-3 IT
    - ImageMASSter 4002i
    - ImageMasster 3002SCSI
    - Image MASSter 3004SATA

Module 61: Windows Based Command Line Tools

- 3Scan
- AGREP
- Aircrack
- ARPFlash
- ASPNetUserPass
- AtNow
- BBIE
- BFI
- Renamer
- BootPart
- BuiltIn Account Manager
- bzip2
- WhoAmI
- Command Line SFV Checker 0.1
- MaxDIR 2.29
- Run! 2.6.7
- Network Ping

- WinTraceRoute
- 4NT 8.02
- Nbtstat
- Netsh
- Taskkill
- Tasklist
- WMIC
- NetStat Agent
- Ping 1.2
- DNS lookup 1.1
- Findstr
- mtsend.py
- wmctrl 1.07
- stsadm
- listadmin (2.40-1)
- Copyprofile
- NBLookup.exe
- Whoiscl
- AccExp
- c2pas32
- fscript 2.0
- GConf
- FMPP
- XQilla
- Mosek
- ToggIT Command Line Helper 1.0
- Bayden SlickRun 2.1
- cb 1.0.0.1
- Blat
- ffmpeg

Module 62: Windows Based GUI Tools

- Process Viewer Tool
  - CurrProcess
  - Process Explorer
  - ProcessMate
  - ServiWin

- Registry Tool
  - Autoruns
  - Autostart Viewer
  - ERUNT
  - Hijackthis
  - Loadorder
  - Regbrws
  - Regedit PE
  - Regscanner
- Desktop Utility Tool
  - BossKey
  - Count Characters
  - HoverSnap
  - Lens
  - Pixie
  - PureText
  - ShoWin
  - Sizer
  - SysExporter
- Office Application Tool:
  - ASCII Values
  - Atlantis Nova
  - Character Grid
  - DateStat
  - DBF Explorer
  - DHB Workshop
  - firstobject XML Editor
  - Foxit PDF Reader
  - Irfan View
  - MetaPad
  - PrintServer
- Remote Control Tool
  - Gencontrol
  - IVT
  - Putty
  - VNC Viewer
- Network Tools

  - Adapterwatch
  - Commtest
  - CurrPorts
  - Hey Joe!
  - IP2
  - IP Netinfo
  - Ldp
  - Necrosoft Dig
  - Net Send (NT Toolkit)
  - POP3 Preview
  - Popcorn
  - Quick Mailer
  - TCPView
  - Trout
  - WinArpSpoof
- Network Scanner Tool
  - Attack Tool Kit(ATK)
  - DDos Ping
  - DNSWalker
  - DSScan
  - GetAcct
  - JJJExec
  - MyDoomScanner
  - Netstumbler
  - RPCScan
  - RPCScan2
  - ShareEnum
  - Shed
  - SNScan
  - SuperScan4
- Network Sniffer Tool
  - Analyzer
  - IPSniffer
  - NGSSniff
  - Show Traffic
  - SmartSniff
  - Sniphere

- Hard Disk Tool
    - 48-bit LBA Technology
    - Darik's Boot and Nuke
    - DirectDisk
    - Disk Checker
    - Disk Investigator
    - DiskMon
    - DiskPatch
    - DiskPie Pro
    - Emsa Disk Check
    - Hard Disk Indicator, HDSpeed
    - HD Tach
    - HD Tune
    - HDClone
    - HDINFO Tool
    - Maxtor MaxBlast
    - Maxtor Powermax
    - MBRtool
    - MBRWork
    - Sectedit
    - Sector Inspector
    - Western Digital Diagnostic
- Hardware Info Tools
    - Bart's Stuff Test
    - Central Brain Identifier
    - Data LifeGuard Diagnostics for Windows
    - Drive View
    - DTemp
    - HD Tune
    - HD_Speed
    - Monitor Test
    - Nero CD/DVD Speed
    - Nero Drive Speed
    - Nero Info Tool
    - ReSysInfo
    - SIW
    - WinAudit

- File Management Tool
    - 1-4a Rename
    - A43
    - CD2ISO
    - Delold
    - Disktools Imagemaker
    - Drvcloner XP, Cdmanipulator
    - Drvimager XP
    - Dscrypt
    - Express Burn
    - Ntouch, Rawwrite for Windows
    - Pablo Commander
    - Pagedefrag
    - Replace in Files, Splitter Light
    - UUD32 Windows
    - Wintidy
- File Recovery Tool
    - Handy Recovery
    - PC Inspector
    - Restoration
    - R-Linux
    - Smart Recovery
    - Zip File Recovery
- File Transfer Tool
    - Babyftp Server
    - Babypop3 Server
    - Babyweb Server
    - Dropupload, File Gateway
    - Dropupload, File Gateway
    - Freeway FTP
    - HFS HTTP File Server
    - Nullsoft Copy, Smbdownloader
    - Simple Socket File Transfer
    - Synchronize It! V1.69
    - TFTPD32
    - Wackget, Thirddir
    - Unstoppable Copier

    - Winscp
- File Analysis Tool
    - AccessEnum
    - BinText
    - CDMage
    - DBF Viewer Plus
    - DefragNT
    - Dependency Walker
    - Disk Investigator
    - DiskView
    - DupeLocator
    - E-Grabber
    - ExamDiff
    - Explore2FS
    - File Analyzer
    - File List Generator
    - Folders Report
    - Gemulator Explorer
    - HashCalc
    - Lister
    - MDB View
    - Media Checker
    - PEiD
    - Resource Hacker
    - Space Monger
    - Tiny Hexer
    - Virtual Floppy Driver
    - Win Interrogate
    - xTeq X-Find
- Password Tool
    - CISCO PIX Firewall Password Calculator
    - Encode Unix Password
    - Password Assistant (NTToolkit)
    - Password Generator
- Password Cracking Tool
    - Access PassView
    - Chat Recovery

  - Asterisk Logger
  - Basic Authentication
  - Brutus
  - DeBat!
  - Dialupass
  - Enterprise Manager PassView
  - GetKey
  - GetPass
  - Keyfinder
  - Lepton’s crack
  - Mail PassView
  - Messenger Key
  - MessenPass
  - Netscapass
  - Outlooker
  - PCAnywhere PassView
  - Protected Storage PassView
  - RockXP
  - Share Password Checker
  - X-Pass
- Other GUI Tools:
  - AtomicTime, FavouritesView
  - IECookiesView
  - IEHistoryView
  - MozillaCookiesViewer
  - MyUninstaller
  - Neutron
  - NewSID
  - ShortCutsMan
  - Timer, Stinger
  - WinUpdatesList
  - DB2 MAESTRO 8.4
  - ORACLE MAESTRO 8.3
  - SQL MAESTRO FOR MYSQL 8.3
  - EMS SQL MANAGER 2007 FOR ORACLE 1.1
  - EMS SQL MANAGER 2005 FOR POSTGRESQL 3.7
  - EMS SQL MANAGER 2008 FOR SQL SERVER 3.0

- EMS SQL MANAGER 2007 FOR POSTGRESQL 4.3
- EMS SQL MANAGER 2008 FOR INTERBASE/FIREBIRD 5.0
- EMS SQL MANAGER FOR DBISAM 1.6
- MS SQL Maestro 8.1
- SQLite Maestro 8.5
- SQLite Data Wizard 8.4
- SQLite Code Factory 7.5
- SQLite PHP Generator 8.1
- Hash 1.04
- Navicat MySQL Manager for Linux 8.0.22

Module 63: Forensics Frameworks

- FORZA Framework
  - What is Forensics Framework?
  - Fundamental Principle in Digital Forensics Investigation Procedures
  - FORZA Framework
  - Roles and Responsibilities of Participants in Digital Forensics Investigation Procedures
  - Process Flow in FORZA Framework
  - High-level View of FORZA Framework
  - FORZA Framework Layers
  - Contextual Investigation Layer
  - Contextual Layer
  - Legal Advisory Layer
  - Conceptual Security Layer
  - Technical Presentation Layer
  - Data Acquisition Layer
  - Data Analysis Layer
  - Legal Presentation Layer
- An Event-Based Digital Forensic Investigation Framework
  - Event-based Framework
  - Digital Analysis Types
  - Digital Investigation Process Model
  - Digital Crime Scene Investigation Phases
- Enhanced Digital Investigation Process Model
  - Enhanced Digital Investigation Process Model
  - Physical Crime Scene Investigation
  - Digital Crime Scene Investigation

  - Phases of Enhanced Digital Investigation Process Model
- Extended Model of Cybercrime Investigations
  - Extended Model of Cybercrime Investigations
  - Activities in Cybercrime Investigations
- Computer Forensics Field Triage Process Model
  - Computer Forensics Field Triage Process Model
  - Computer Forensics Field Triage Process Model Phases
- Objectives-Based Framework for the Digital Investigations Process
  - Objectives-based Framework
  - Proposed Digital Investigation Process
  - Objectives-Based Framework Phases

Module 64: Forensics Investigation Templates

- Case Feedback Form
- Seizure Record
- List of Evidence Gathered Form
- Evidence Preservation Checklist
- BIOS Configuration
- System Configuration
- Application Summary
- Monitor Investigation Checklist
- Hard Disk Investigation Checklist
- Floppy Investigation Checklist
- CD Investigation Checklist
- Zip Drive Investigation Checklist
- Flash Drives Investigation Checklist
- Tape Investigation Checklist
- Handheld Device Investigation Checklist: Blackberry
- Handheld Device Investigation Checklist: iPod
- Handheld Device Investigation Checklist: Mobile Phone
- Handheld Device Investigation Checklist: PDA
- Fax Investigation Checklist
- Hub Investigation Checklist
- Switch Investigation Checklist
- Router Investigation Checklist
- Physical Security Checklist

- Identity Theft Checklist

Module 65: Computer Forensics Consulting Companies

- Burgess Forensics
- Center for Computer Forensics (CCF)
- Navigant Consulting
- ACR Data Recovery
- Computer Forensic Services
- Cyber Evidence Inc.
- Data Recon
- ADR (American Data Recovery) Computer Forensics
- Berryhill Computer Forensics, Inc.
- CIA Solutions
- Federal Bureau of Investigation (FBI)
- Interpol
- National Center for Missing and Exploited Children (NCMEC)
- Logicube
- Logicube: Screenshot
- LJ Forensics
- Intelligent Computer Solutions (ICS)
- Intelligent Computer Solutions (ICS): Screenshot
- Cy4or
- Forensicon
- Global Digital Forensics
- Integrity Security & Investigation Services, Inc. (ISIS)
- Trial Solutions
- Digital Detective
- Florida Department of Law Enforcement
- Northern California Computer Crimes Task Force (NC3TF)
- Child Exploitation and Online Protection Centre (CEOP)
- eFrauda
- International Association of Computer Investigative Specialists (IACIS)
- 7Safe
- Adroit Infotech Consultancy Service
- Digital Medix
- Hill Schwartz Spilker Keller LLC (HSSK)
- IRIS Data Services

- Computer Forensic Labs, Inc.